ELEMENTARY NUMBER THEORY

DAVID PIERCE

These notes are based on my lectures, in the fall of 2007, in Elementary Number Theory (Math 365). I wrote from memory and from the handwritten notes that I used during the lectures. The main reference for the course was [1], but I used also [3]. The Tuesday lectures were two hours; Thursday, one. (Each hour is 50 minutes.)

There were three in-term examinations, on October 23 (Tuesday), November 27 (Tuesday), and December 27 (Thursday). On those days in class, I introduced no new material. Class was cancelled November 13 and 15, because was at the Centre Internationale de Rencontres Mathématiques. October 11 (Thursday) fell within the *Şeker Bayramı;* December 20 (Thursday), the *Kurban Bayramı.*

As the semester progressed, I made available on the web some notes (with exercises) called 'Foundations of number-theory' [7], along with ten more sets of exercises.

Contents

Date: January 11, 2008.

1. September 20, 2007 (Thursday)

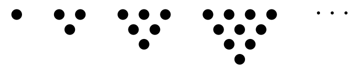
What can we say about the sequence

$$3, 6, 10, 15, 21, 28, \ldots?$$

We can add a couple of terms to the beginning, making it

$$0, 1, 3, 6, 10, 15, 21, 28, \ldots$$

The terms increase by 1, 2, 3, and so on. What do the numbers *look like?* They are the **triangular numbers:**



Let $t_0 = 0$, $t_1 = 1$, $t_2 = 3$, &c. The **recursive** definition is

$$t_0 = 0, \quad t_{n+1} = t_n + n + 1.$$

There is a *closed* form:

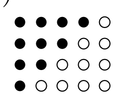
$$t_n = \sum_{k=1}^{n} k = \binom{n+1}{2} = \frac{n(n+1)}{2}. \tag{$*$}$$

We can prove this by **induction:** It is true when $n = 0$ (or $n = 1$), and if it is true when $n = k$, then

$$t_{k+1} = t_k + k + 1 = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

so it is true when $n = k + 1$. By induction, $(*)$ is true for all n.

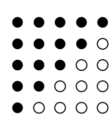
But *why* is equation $(*)$ true? This can be seen from a picture: two copies of t_n fit together to make a rectangle of $n(n+1)$ dots:



Similarly, $(n+1)^2 = t_{n+1} + t_n$, since

$$t_{n+1} + t_n = \frac{(n+1)(n+2)}{2} + \frac{n(n+1)}{2} = \frac{n+1}{2}(n + 2 + n) = (n+1)^2;$$

but this can be seen in a picture:



What can we say about the following sequence?

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, \ldots$$

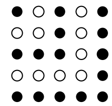
It is the sequence of odd numbers. Also, the first n terms seem to add up to n^2, that is,

$$n^2 = \sum_{k=1}^{n} (2k - 1). \tag{$\dagger$}$$

We can prove this by induction: It is true when $n = 0$, and if it is true when $n = k$, then

$$(k+1)^2 = k^2 + 2k + 1 = \sum_{j=1}^{k} (2j - 1) + 2k + 1 = \sum_{j=1}^{k+1} (2j - 1),$$

so it is true when $n = k + 1$. Therefore $(\dagger)$ is true for all n. A picture shows why:



Finally, observe:

$$1, \underbrace{3, 5}_{8}, \underbrace{7, 9, 11}_{27}, \underbrace{13, 15, 17, 19}_{64}, \underbrace{21, 23, 25, 27, 29}_{125}, \dots$$

Does the pattern continue? As an exercise, write the suggested equation,

$$n^3 = \sum_{\dots}^{\dots} \dots,$$

and prove it. (The theorem was apparently known to Nicomachus of Gerasa [6, II.20.5, p. 263], almost 2000 years ago.)

*   *   *   *   *

We are studying the natural numbers, 0, 1, 2, ... (Some people start with 1 instead.) They compose the set $\mathbb{N}$. Everything about $\mathbb{N}$ follows from the following five conditions:

(a) there is a first natural number, **zero** (0);
(b) each n in $\mathbb{N}$ has a **successor**, $\mathrm{s}(n)$;
(c) 0 is not a successor;
(d) distinct numbers have distinct successors: if $n \neq m$, then $\mathrm{s}(n) \neq \mathrm{s}(m)$;
(e) **induction:** if $A \subseteq \mathbb{N}$, and
  (i) $0 \in A$, and
  (ii) if $n \in A$, then $\mathrm{s}(n)$ is in A,
 then $A = \mathbb{N}$.

2. September 25, 2007 (Tuesday)

Theorem (Recursion). *Suppose A is a set with an element b, and $f : A \to A$. Then there is a* unique *function g from $\mathbb{N}$ to A such that*

(a) *$g(0) = b$, and*
(b) *$g(\mathrm{s}(n)) = f(g(n))$ for all n in $\mathbb{N}$.*

For the proof, see [7]. By recursion, we define addition and multiplication:

$$m + 0 = m, \qquad m \cdot 0 = 0,$$
$$m + \mathrm{s}(n) = \mathrm{s}(m + n), \qquad m \cdot \mathrm{s}(n) = m \cdot n + m.$$

Then the usual properties can be proved, usually by induction (exercise; see [7]). We write 1 for $\mathrm{s}(0)$, so $\mathrm{s}(n) = n + 1$.

Some books suggest wrongly that everything about $\mathbb{N}$ is a consequence of:

Theorem (Well-Ordering Principle). *Every non-empty subset of $\mathbb{N}$ has a least element.*

But what does *least* mean? The **least** element of A is some n such that

(a) $n \in A$;
(b) if $m \in A$, then $n \leqslant m$.

On $\mathbb{N}$, we define $\leqslant$ by

$$m \leqslant n \iff m + k = n \text{ for some } k \text{ in } \mathbb{N}.$$

Again, the usual properties can be proved (exercise; see [7]).

Let's try to prove the WOP (the Well-Ordering Principle). Suppose $A \subseteq \mathbb{N}$, and A has no least element. We want to show that A is empty, that is, $\mathbb{N} \smallsetminus A = \mathbb{N}$. Try induction. For the base step, we cannot have $0 \in A$, since then 0 would be the least element of A. So $0 \notin A$.

For the inductive step, suppose $n \notin A$. This is not enough to establish $n+1 \notin A$, since maybe $n-1 \in A$, so $n+1$ can be in A without being least.

We need:

Theorem (Strong Induction)**.** *Suppose $A \subseteq \mathbb{N}$, and for all n in $\mathbb{N}$, if all predecessors of n belong to A, then $n \in A$. Then $A = \mathbb{N}$.*

For the proof, see [7]. Now we can prove well-ordering: If A has no least element, and no member of the set $\{x \in \mathbb{N} \colon x < n\}$ belongs to A, then A must not belong either. Therefore, by strong induction, $A = \varnothing$.

* * * * *

Our course is Elementary Number Theory. Here 'elementary' does not mean easy; it means not involving mathematical analysis. For example, although the function given by

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} \,\mathrm{d}\, x$$

satisfies $\Gamma(n+1) = n\Gamma(n)$, and $\Gamma(1) = 1$, so that $G(n+1) = n!$, we shall not study such facts.

* * * * *

Our main object of study is the **integers,** which compose the set

$$\mathbb{N} \cup \{-x \colon x \in \mathbb{N} \smallsetminus \{0\}\},$$

denoted by $\mathbb{Z}$. Then we extend addition and multiplication and the ordering to $\mathbb{Z}$, and we define additive inversion on $\mathbb{Z}$, so that

$$\begin{aligned}
a + (b + c) &= (a + b) + c & \qquad a \cdot (b \cdot c) &= (a \cdot b) \cdot c,\\
b + a &= a + b, & b \cdot a &= a \cdot b,\\
a + 0 &= a, & a \cdot 1 &= a,\\
a + (-a) &= 0,
\end{aligned}$$

$$\begin{gathered}
a \cdot (b + c) = a \cdot b + a \cdot c,\\
a < b \Rightarrow a + c < b + c,\\
0 < a \;\&\; 0 < b \Rightarrow 0 < a \cdot b.
\end{gathered}$$

So $\mathbb{Z}$ is an **ordered domain** (but it is not necessary to know this term).

If $a \in \mathbb{Z}$, let the set $\{ax \colon x \in \mathbb{Z}\}$ be denoted by $\mathbb{Z}a$ or $a\mathbb{Z}$ or

$$(a).$$

Then $b \in (a)$ if and only if a **divides** b, which is denoted by

$$a \mid b.$$

If $c - b \in (a)$, then we may also write

$$b \equiv c \pmod{a} :$$

b and c are **congruent *modulo*** a. Congruence is an equivalence-relation. The congruence-class of b *modulo* a is

$$\{x \in \mathbb{Z} \colon b - x \in (a)\}.$$

How many congruence-classes *modulo* a are there?

If $a = 0$, then congruence *modulo* a is equality. Otherwise, there are $|a|$ congruence-classes *modulo* a, namely the classes of 0, $1, \dots, |a| - 1$. This is by:

Theorem (Division). *If $a \neq 0$, and $b \in \mathbb{Z}$, then the system*

$$b = ax + y \ \&\ 0 \leqslant y < |a|$$

has a unique solution.

Proof. The set $\{z \in \mathbb{N} \colon z = b - ax \text{ for some } x \text{ in } \mathbb{Z}\}$ is non-empty (why?). Let r be its least element, and let q be such that $r = b - aq$. Then $b = aq + r$ and $0 \leqslant r < |a|$. □

Consequently, every square has the form $3n$ or $3n + 1$. Indeed, every number is $3k$ or $3k + 1$ or $3k + 2$, and

$$\begin{gathered}(3k)^2 = 9k^2 = 3(3k^2),\\ (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1,\\ (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.\end{gathered}$$

Alternatively, since ongruent numbers have congruent squares,

$$\begin{gathered}0^2 = 0,\\ 1^2 = 1,\\ 2^2 = 4 \equiv 1 \pmod 3.\end{gathered}$$

Similarly, every cube is $7n$ or $7n \pm 1$, since

$$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8 = 7 + 1 \equiv 1 \pmod 7, \quad \dots$$

Facts about divisibility:

$$\begin{gathered}a \mid 0;\\ 0 \mid a \iff a = 0;\\ 1 \mid a \ \&\ a \mid a;\\ a \mid b \ \&\ b \neq 0 \Rightarrow |a| \leqslant |b|;\\ a \mid b \ \&\ b \mid c \Rightarrow a \mid c\\ a \mid b \ \&\ c \mid d \Rightarrow ac \mid bd;\\ a \mid b \Rightarrow a \mid bx; \qquad (*)\\ a \mid b \ \&\ a \mid c \Rightarrow a \mid b + c. \qquad (\dagger)\end{gathered}$$

By the last two implications, $(*)$ and $(\dagger)$, if $a \mid b$ and $a \mid c$, then a divides every **linear combination**

$$ax + by$$

of a and b. Let the set $\{ax + by \colon x, y \in \mathbb{Z}\}$ of these linear combinations be denoted by

$$(a, b).$$

Then $(0, 0) = (0)$. Otherwise, assuming one of a and b is not 0, let n be the least positive element of (a, b). Then n divides a and b. Indeed, $a = nq + r$ and $0 \leqslant r < n$ for some q and r. Then $r = a - nq = a - (ax + by)q = a(1 - qx) + b(-qy)$ for some x and y, so $r \in (a, b)$, and hence $r = 0$ by minimality of n, so $n \mid a$. Similarly, $n \mid b$.

Then n is the *greatest* common divisor of a and b. Why? If $d \mid a$ and $d \mid b$, then $d \mid n$, since n is a linear combination of a and b; so $d \leqslant |d| \leqslant |n| = n$. Therefore n is the **greatest common divisor** of a and b:

$$n = \gcd(a, b).$$

We have also

$$(a, b) = (n)$$

(so $\mathbb{Z}$ is a **principal ideal domain**). Indeed, immediately, $(n) \subseteq (a, b)$. Also, as n divides a and b, it divides every element of (a, b), so $(a, b) \subseteq (n)$.

If $\gcd(a, b) = 1$, then a and b are **relatively prime** or **co-prime.** So this is the case if and only if the equation

$$ax + by = 1$$

has a solution.

In general, if $\gcd(a, b) = n$, then

$$\gcd\left(\frac{a}{n}, \frac{b}{n}\right) = 1,$$

since both $ax + by = n$ and $(a/n)x + (b/n)y = 1$ have solutions.

Suppose a and b are co-prime, and each divides c; then so does ab. Indeed, the following have solutions:

$$\begin{aligned} ax + by &= 1, \\ acx + bcy &= c, \\ absx + bary &= c, \\ ab(sx + ry) &= c, \end{aligned}$$

where $c = bs = ar$.

Lemma (Euclid, VII.30)**.** *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Again, the following have solutions:

$$\begin{aligned} ax + by &= 1, \\ acx + bcy &= c. \end{aligned}$$

Since $a \mid ac$ and $a \mid bc$, we are done. □

* * * * *

How can we find solutions to an equation like the following?

$$63x + 7 = 23y.$$

Rewrite as

$$63x - 23y = -7.$$

For a solution, we must have

$$\gcd(63, 23) \mid 7.$$

But how do we know what the gcd *is?*

3. September 27, 2007 (Thursday)

Recall that $(a,b) = \{\text{linear combinations of } a \text{ and } b\}$; its least positive element (if one of a and b is not 0) is $\gcd(a,b)$. Let this be n. We showed

$$(a,b) = (n). \tag{$*$}$$

The set $(a) \cap (b)$ consists of the common multiples of a and b; so its least positive element is the **least common multiple** of a and b, or

$$\operatorname{lcm}(a,b).$$

Suppose this is m. As we showed $(*)$, so we can show

$$(a) \cap (b) = (m).$$

For example,

$$\begin{tikzcd} & \operatorname{lcm}(10,15) = 30 \arrow[dl, dash] \arrow[dr, dash] & \\ 10 \arrow[dr, dash] & & 15 \arrow[dl, dash] \\ & \gcd(10,15) = 5 & \end{tikzcd}$$

Note $5 \cdot 30 = 10 \cdot 15$. In general, since $ab \in (a) \cap (b)$, we have

$$\operatorname{lcm}(a,b) \mid ab. \tag{$\dagger$}$$

Theorem. $\gcd(a,b)\operatorname{lcm}(a,b) = |ab|$.

Proof. Let $n = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. We can solve

$$\begin{aligned} ax + by &= n, \\ amx + bmy &= mn. \end{aligned}$$

But $a, b \mid m$, so $ab \mid am, bm$, so $ab \mid mn$, hence

$$|ab| \leqslant mn. \tag{$\ddagger$}$$

Also, $m = ar = bs$ for some r and s; and $\gcd(r,s) = 1$ by minimality of m as a divisor of a and b. Hence we can solve

$$\begin{aligned} sx + ry &= 1, \\ absx + abry &= ab, \\ amx + bmx &= ab, \\ ax + by &= \frac{ab}{m} \end{aligned}$$

(using $(\dagger)$). As $n \mid a, b$, so $n \mid ab/m$, and hence

$$|n| \leqslant \frac{|ab|}{m}$$

(assuming $ab \neq 0$), so $mn \leqslant |ab|$. By this and $(\ddagger)$, $mn = |ab|$. ∎

* * * * *

How can we *find* $\gcd(a,b)$? The **Euclidean algorithm.** What is it? For example, $\gcd(9,12)=3$, by

$$\begin{aligned} 12 &= 9\cdot 1+3,\\ 9 &= 3\cdot 3+0. \end{aligned}$$

In general, suppose $a_0 > a_1 \geqslant 0$. By *strong* recursion, define a_2, a_3,... by

$$a_n = a_{n+1}q + a_{n+2} \ \&\ 0 \leqslant a_{n+2} < a_{n+1} \tag{§}$$

(for some q) if $a_{n+1} \neq 0$; but if $a_{n+1}=0$, then let $a_{n+2}=0$. Then the descending sequence

$$a_0 > a_1 > a_2 > \cdots$$

must stop. That is, let a_m be the least element of $\{a_n \colon a_n > 0\}$, so that $a_{m+1}=0$. Then

$$\gcd(a_0,a_1)=a_m;$$

why? Because, if $a_{n+1}\neq 0$, then $\gcd(a_n,a_{n+1})=\gcd(a_{n+1},a_{n+2})$ by (§); so, by induction,

$$\gcd(a_0,a_1)=\gcd(a_1,a_2)=\cdots=\gcd(a_m,a_{m+1})=\gcd(a_m,0)=a_m.$$

* * * * *

A cock costs 5 L; a hen, 3 L; 3 chicks, 1 L. Can we buy 100 birds with 100 L? Let

$$\begin{aligned} x &= \#\text{ cocks},\\ y &= \#\text{ hens},\\ z &= \#\text{ chicks}. \end{aligned}$$

We want to solve

$$\begin{aligned} x+y+z &= 100,\\ 5x+3y+\frac{1}{3}z &= 100. \end{aligned} \tag{¶}$$

Eliminate z and proceed:

$$\begin{aligned} z &= 100-x-y,\\ 15x+9y+z &= 300,\\ 15x+9y+100-x-y &= 300,\\ 14x+8y &= 200,\\ 7x+4y &= 100. \end{aligned} \tag{‖}$$

Since $4 \mid 100$, one solution is $(0,25)$, that is, $x=0$ and $y=25$. Then $y=75$. So the answer to the original question is Yes. But can we include at least one cock? What are all the solutions?

Think of linear algebra. If (x_0,y_0) and (x_1,y_1) are two solutions to (‖), then

$$\begin{aligned} 7x_0+4y_0 &= 100,\\ 7x_1+4y_1 &= 100,\\ 7(x_1-x_0)+4(y_1-y_0) &= 0. \end{aligned}$$

So we want to solve

$$7x+4y=0.$$

Since $\gcd(7,4)=0$, the solutions are $(4t,-7t)$. (Here is a difference with the usual linear algebra.) So the original system (¶) has the general solution

$$(x,y,z)=(4t,25-7t,75+3t).$$

If we want all entries to be positive, this means

$$4t>0,\quad 25-7t>0,\quad 75+3t>0;$$
$$t>0,\quad 7t<25,\quad 3t>-75;$$
$$0<t<\frac{25}{7};$$
$$0<t\leqslant 3.$$

So there are three solutions:

x	y	z
4	18	78
8	11	81
12	4	88

4. October 2, 2007 (Tuesday)

A curiosity (from 'On Teaching Mathematics' by V. I. Arnold):

$$\begin{aligned}
&1,\\
&3=1+1+1,\\
&5=3+1+1=2+2+1=1+1+1+1+1,\\
&7=5+1+1=4+2+1=3+3+1=3+2+2=\\
&\quad=3+1+1+1=2+2+1+1+1=1+1+1+1+1+1+1,\\
&9=\cdots.
\end{aligned}$$

Write the odd numbers as sums of odd numbers of summands. Then we have

n	# sums for n
1	1
3	2
5	4
7	8
9	16
11	29

Thus the pattern $2^0,2^1,2^2,\dots$ breaks down. Is there a formula for the sequence of numbers of sums?

* * * * *

A positive integer is **prime** if it has exactly two distinct positive divisors. So, 1 is not prime. Also, p is prime if and only if $p>1$ and

$$a\mid p\Rightarrow |a|\in\{1,p\}.$$

Let p and q always stand for primes. Then

$$\gcd(a,p)\in\{1,p\},$$

so either a and p are co-prime, or else $p\mid a$.

Suppose $p\mid ab$. Either $p\mid a$, or else $\gcd(a,p)=1$, so $p\mid b$ by Euclid's Lemma. Hence, by induction, if $p\mid a_0\cdots a_n$, then $p\mid a_k$ for some k. Indeed, the claim is true when n is

0 or 1. Suppose it is true when $n = m$. Say $p \mid a_0 \cdots a_{m+1}$. By the case $n = 1$, we have that $p \mid a_0 \cdots a_m$ or $p \mid a_{m+1}$. In the former situation, by the inductive hypothesis, $p \mid a_k$ for some k. So the claim holds when $n = m + 1$.

Theorem (Fundamental, of Arithmetic)**.** *Every positive integer is uniquely a product*

$$p_1 \cdots p_n$$

of primes, where

$$p_1 \leqslant \cdots \leqslant p_n.$$

Proof. Note that 1 is such a product, where $n = 0$. Suppose $m > 1$. Let p_1 be the least element of $\{x \in \mathbb{N} \colon x > 1 \mathbin{\&} x \mid m\}$. Then p_1 must be prime; otherwise, if $a \mid p_1$, and $a > 0$, but $a \notin \{1, p\}$, then $1 < a < p$, but $a \mid m$, so the minimality of p_1 is contradicted. Now let p_2 be the least prime divisor of m/p_1, and so forth. We have

$$m > \frac{m}{p_1} > \frac{m}{p_1 p_2} > \cdots$$

This must terminate in

$$\frac{m}{p_1 \dots p_n} = 1$$

by the Well-Ordering Principle, so that $m = p_1 \cdots p_n$.

For uniqueness, suppose also $m = q_1 \cdots q_\ell$. Then $q_1 \mid m$, so $q_1 \mid p_i$ for some i, and therefore $q_1 = p_i$. Hence

$$p_1 \leqslant p_i = q_1.$$

By the symmetry of the argument, $q_1 \leqslant p_1$, so $p_1 = q_1$. Similarly, $p_2 = q_2$, &c., and $n = \ell$. □

An analogous statement fails in some similar contexts. For example,

$$(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 2 \cdot 3;$$

but among the numbers $a + b\sqrt{10}$, the numbers $4 \pm \sqrt{10}, 2, 3$ are "irreducible" (like primes). Such matters are studied in *algebraic* number theory.

A positive non-prime number is **composite** if it has prime factors. Then every positive number is uniquely prime, composite, or 1.

* * * * *

Theorem. *The equation*

$$x^2 = 2y^2$$

has no non-zero solution.

Proof. Suppose $a^2 = 2b^2$. Then $2 \mid a^2$, so $2 \mid a$, so $4 \mid a^2$, so $4 \mid 2b^2$, so $2 \mid b^2$, so $2 \mid b$. But if a and b are not 0, then we may assume they are co-prime (otherwise, replace them with a/d and b/d, where $d = \gcd(a, b)$). So a and b must be 0. □

* * * * *

One can find primes with the Sieve of Eratosthenes... Eratosthenes also measured the circumference of the earth, by measuring the shadows cast by posts a certain distance apart in Egypt. Measuring *this* distance must have needed teams of surveyors and a government to fund them. Columbus was not in a position to make the measurement again, so he had to rely on ancient measurements [8].

* * * * *

Theorem (Euclid, IX.20). *If $n \in \mathbb{N}$, then there are more than n primes.*

Proof. Suppose $p_0 < \cdots < p_{n-1}$, all prime. Then $p_0 \cdots p_{n-1} + 1$ has a prime factor, distinct from the p_k. □

An alternative argument by Filip Saidak (2005) is reported in the latest *Matematik Dünyası:* Define $a_0 = 2$ and $a_{n+1} = a_n(1 + a_n)$. If $k < n$, then $a_k \mid a_{k+1}$, and $a_{k+1} \mid a_{k+2}$, and so on, up to $a_{n-1} \mid a_n$, so $a_k \mid a_n$. Similarly, since $1 + a_k \mid a_{k+1}$, we have $1 + a_k \mid a_n$. Therefore $\gcd(1+a_k, 1+a_n) = 1$. Thus any two elements of the infinite set $\{1+a_n : n \in \mathbb{N}\}$ are co-prime.

* * * * *

I state some theorems, without giving proofs; some of them are recent and reflect ongoing research:

Theorem (Dirichlet). *If $\gcd(a, b) = 1$, and $b > 0$, then $\{a+bn : n \in \mathbb{N}\}$ contains infinitely many primes.*

That is, arithmetic progressions (with the obvious condition...) contain infinitely many primes.

The textbook [1] omits the following.

Theorem (Ben Green and Terence Tao [5], 2004). *For every n, there are a and b such that each of the numbers $a, a + b, a + 2b, \dots, a_nb$ is prime (and $b > 0$).*

That is, there are arbitrarily long arithmetic progressions of primes.

Is it possible that each of the numbers

$$a, a + b, a + 2b, a + 3b, \dots$$

is prime? Yes, if $b = 0$. What if $b > 0$? Then No, since $a \mid a + ab$. But what if $a = 1$? Then replace a with $a + b$.

Two primes p and q are **twin** if $|p - q| = 2$. The list of all primes begins:

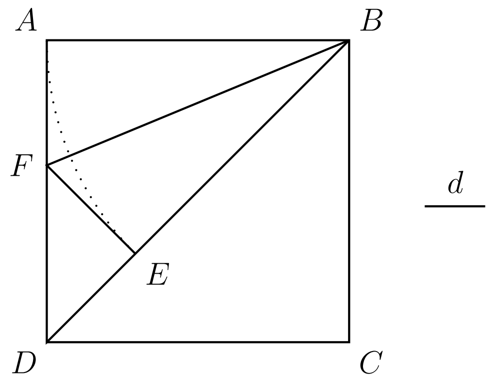
$$2, \underbrace{3, 5}, \underbrace{5, 7}, \underbrace{11, 13}, \underbrace{17, 19}, 23, \underbrace{29, 31}, 37, \underbrace{41, 43}, 47, \dots$$

and there are several twins. Are there infinitely many? People think so, but can't prove it. We do have:

Theorem (Goldston, Pintz, Yıldırım [4], 2005). *For every positive real number ε, there are primes p and q such that $0 < q - p < \varepsilon \cdot \ln p$.*

* * * * *

I return to the irrationality of $\sqrt{2}$ (there is no non-zero solution to $x^2 = 2y^2$). Geometrically, the claim is that the side and diagonal of a square are **incommensurable:** there is no line segment that evenly divides them. We can see this as follows [2, v. I, p. 19]:



Let $ABCD$ be a square. On the diagonal BD, mark BE equal to AB. Let the perpendicular at E meet AD at F. Draw BF. Then triangles ABF and EBF are congruent, so $EF = AF$. Also, DEF is an isosceles right triangle, so $DE = EF$. Suppose d measures both AB and BD. Then it measures ED and DF, since

$$\begin{aligned} ED &= BD - AB, \\ DF &= AB - ED. \end{aligned}$$

Now do the same construction to DEF in place of DAB. Since $2ED < AB$, we eventually get segments that are shorter than d, but are measured by it, which is absurd. So such d cannot exist.

This argument can be made more algebraic. We have

$$1 = 2 - 1 = (\sqrt{2})^2 - 1^2 = (\sqrt{2}+1)(\sqrt{2}-1),$$

so

$$\sqrt{2} + 1 = \frac{1}{\sqrt{2}-1}.$$

Then

$$\begin{aligned} \sqrt{2}+1 &= 1 \cdot 2 + (\sqrt{2}-1), \\ 1 &= (\sqrt{2}-1) \cdot 2 + (3 - 2\sqrt{2}), \\ \sqrt{2}-1 &= \cdots . \end{aligned}$$

That is, if we let $a_0 = \sqrt{2}+1$ and $a_1 = 1$, then we can define

$$a_n = a_{n+1} \cdot 2 + a_{n+2}.$$

So we have

$$\begin{aligned} a_0 &= a_1 \cdot 2 + a_2, \\ a_1 &= a_2 \cdot 2 + a_3, \\ a_2 &= a_3 \cdot 2 + a_4, \end{aligned}$$

and so on. Then

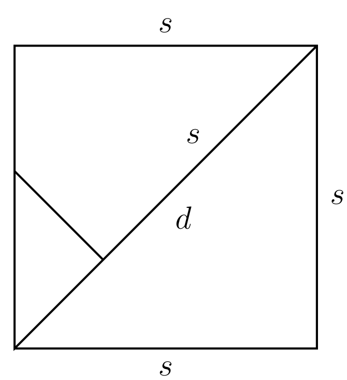
$$\frac{a_0}{a_1} = 2 + \frac{a_2}{a_1} = 2 + \cfrac{1}{\cfrac{a_1}{a_2}} = 2 + \cfrac{1}{2 + \cfrac{a_3}{a_2}} = 2 + \cfrac{1}{2 + \cfrac{1}{\cfrac{a_2}{a_3}}} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{a_4}{a_3}}} = \cdots ,$$

which means

$$\sqrt{2}+1=2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}}} \tag{$*$}$$

5. October 4, 2007 (Thursday)

Last time we obtained $(*)$ by the Euclidean Algorithm.



Let d and s be the diagonal and side of a square. Then we have

$$\frac{d+s}{s}=\frac{s}{d-s}$$

since $d^2-s^2=s^2$. Applying the Algorithm, we have

$$\begin{aligned} d+s &= s\cdot 2+d-s,\\ s &= (d-s)\cdot 2+\cdots,\\ d-s &= \cdots 2+\cdots, \end{aligned}$$

so that

$$\frac{d+s}{s}=2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}$$

Compare with an ordinary application of the Algorithm. What is $\gcd(134,35)$? We have

$$\begin{aligned} 134 &= 35\cdot 3+29,\\ 35 &= 29\cdot 1+6,\\ 29 &= 6\cdot 4+5,\\ 6 &= 5\cdot 1+1,\\ 5 &= 1\cdot 5. \end{aligned}$$

Therefore $\gcd(134, 35) = 1$; but what is the significance of the numbers 3, 1, 4, 1, 5? They appear in the continued fraction:

$$\frac{134}{35} = 3 + \frac{29}{35} = 3 + \cfrac{1}{\cfrac{35}{29}} = 3 + \cfrac{1}{1 + \cfrac{6}{29}} = 3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{29}{6}}}$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{5}{6}}} = 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\cfrac{6}{5}}}} = 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

* * * * *

Let $\mathbb{P}$ be the set of primes; an alternative proof of its infinity, using the full Fundamental Theorem of Arithmetic, is as follows. Consider the product

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p}}.$$

If $\mathbb{P}$ is finite, then so is this product. But what can we say about $\dfrac{1}{1-\frac{1}{p}}$? We have

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots = \sum_{k=0}^{\infty} \frac{1}{p^k}.$$

Hence

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p}} = \prod_{p\in\mathbb{P}} (1 + \frac{1}{p} + \frac{1}{p^2} + \cdots).$$

Alternatively, if $\mathbb{P} = \{p_1, p_2, \dots\}$, then this product is

$$\left(1 + \frac{1}{p_1} + \frac{1}{{p_1}^2} + \cdots\right) \cdot \left(1 + \frac{1}{p_1} + \frac{1}{{p_1}^2} + \cdots\right) \cdots$$

which is the sum of terms

$$\frac{1}{{p_0}^{e(0)}{p_1}^{e(1)} \cdots p_n^{e(n)}},$$

where $e(i) \geqslant 0$. Rather, the product is the sum of terms

$$\frac{1}{{q_0}^{f(0)}{q_1}^{f(1)} \cdots {q_{m-1}}^{f(m-1)}},$$

where q_i are prime and $f(i) > 0$. But every positive integer is *uniquely* a product ${q_0}^{f(0)}{q_1}^{f(1)} \cdots {q_{m-1}}^{f(m-1)}$, by the Fundamental Theorem. Therefore

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}.$$

If $\mathbb{P}$ is infinite, then we must talk about convergence; but if $\mathbb{P}$ is finite, there is no problem. But the harmonic series $\sum_{n=1}^{\infty}\frac{1}{n}$ diverges:

$$1+\frac{1}{2}+\underbrace{\frac{1}{3}+\frac{1}{4}}_{\geqslant\frac{1}{2}}+\underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}_{\geqslant\frac{1}{2}}+\cdots$$

Therefore $\mathbb{P}$ must be infinite. Using similar ideas, one can show that $\sum_{p\in\mathbb{P}}\frac{1}{p}$ diverges.

* * * * *

Suppose $p\in\mathbb{P}$. If $p\mid ab$, but $p\nmid a$, then $p\mid b$.

If $p=ab$, but $p\nmid a$, then $p\mid b$, but also $b\mid p$, so $b=\pm p$, and then $a=\pm1$.

Among the integers, what property do 1 and -1 have uniquely? They have multiplicative inverses:

$$(-1)\cdot(-1)=1,\qquad 1\cdot 1=1,$$

but if $|n|>1$, then the equation $nx=1$ has no solution. In a word, ±1 are **units** in $\mathbb{Z}$. Then an integer n is called **irreducible** if

(a) $n=ab\Rightarrow(a$ or b is a unit$)$;
(b) n is not a unit.

Then the irreducibles of $\mathbb{Z}$ are $\pm p$, where p is prime.

But irreducibility of primes is not enough to prove *uniqueness* of prime factorizations. If

$$p_1\cdots p_m=q_1\cdots q_n,$$

where $p_1\leqslant\cdots p_m$ and $q_1\leqslant\cdots q_m$, how do we know $p_1=q_1$, &c.? We need the stronger property that $p\mid ab\Rightarrow(p\mid a$ or $p\mid b)$.

Again, there is a situation where the stronger property fails for arbitrary irreducibles:

$$(4+\sqrt{10})(4-\sqrt{10})=6=2\cdot 3,$$

but $4\pm\sqrt{10}$, 2, and 3 are irreducible in $\{x+y\sqrt{10}\colon x,y\in\mathbb{Z}\}$, which is denoted by $\mathbb{Z}[\sqrt{10}]$. Let $\sigma\colon\mathbb{Z}[\sqrt{10}]\to\mathbb{Z}[\sqrt{10}]$, where

$$\sigma(a+b\sqrt{10})=a-b\sqrt{10}.$$

(Compare this with complex conjugation.) Now define $N(x)=x\cdot\sigma(x)$, so that

$$N(a+b\sqrt{10})=a^2-10b^2.$$

Then one can show $N(xy)=N(x)\cdot N(y)$. Also, $N(c)$ is always a square *modulo* 10. We have

$$\begin{aligned}
&0^2=0,\\
&1^2=1,\\
&2^2=4,\\
&3^2=9\equiv-1\pmod{10},\\
&4^2=16\equiv-4\pmod{10},\\
&5^2=25\equiv5\pmod{10},
\end{aligned}$$

so $N(c)$ is congruent to 0, ±1, ±4 or 5 *modulo* 10.

6. October 9, 2007 (Tuesday)

We have implicitly used that congruence respects arithmetic: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{n}, \\ a \cdot c &\equiv b \cdot d \pmod{n}. \end{aligned}$$

Indeed, we assume $n \mid b - a$ and $n \mid d - c$, so $n \mid b - a + d - c$, that is,

$$n \mid b + d - (a + c),$$

which means $a+c \equiv b+d \ (n)$; likewise, $n \mid (b-a)c+(d-c)b$, that is, $n \mid bd-ac$, so $ac \equiv bd$ (n). In short, if set $\mathbb{Z}/(n)$ or $\mathbb{Z}_n$ of congruence-classes *modulo* n is a **commutative ring.**

Hence we can solve $35^{14} \equiv x \ (43)$ as follows: First, $35 \equiv -8 \ (43)$, so

$$35^{14} \equiv (-8)^{14} \equiv 8^{14} \quad (43).$$

Also, $14 = 8 + 4 + 2 = 2^3 + 2^2 + 2^1$, so $8^{14} = 8^8 \cdot 8^4 \cdot 8^2$; and

$$\begin{aligned} 8^2 &= 64 \equiv 21 \quad (43), \\ 21^2 &= 441 \equiv 11 \quad (43), \\ 11^2 &= 121 \equiv 35 \equiv -8 \quad (43), \end{aligned}$$

so that

$$\begin{aligned} 35^{14} &\equiv -8 \cdot 11 \cdot 21 \quad (43) \\ &\equiv -88 \cdot 21 \quad (43) \\ &\equiv -2 \cdot 21 \quad (43) \\ &\equiv -44 \equiv 1 \quad (43). \end{aligned}$$

* * * * *

For another use of congruences, recall $\mathbb{Z}[\sqrt{10}] = \{x + y\sqrt{10} \colon x, y \in \mathbb{Z}\}$, closed under addition and multiplication; and

$$\begin{aligned} \sigma \colon \mathbb{Z}[\sqrt{10}] &\longrightarrow \mathbb{Z}[\sqrt{10}], \\ x + y\sqrt{10} &\longmapsto x - y\sqrt{10}, \end{aligned}$$

and

$$\begin{aligned} N \colon \mathbb{Z}[\sqrt{10}] &\longrightarrow \mathbb{Z}, \\ x &\longmapsto x \cdot \sigma(x). \end{aligned}$$

Then $N(ab) = N(a) \cdot N(b)$. If a is a unit (that is, invertible) of $\mathbb{Z}[\sqrt{10}]$, then $ab = 1$ for some b in $\mathbb{Z}[\sqrt{10}]$, so $N(ab) = N(1)$, that is, $N(a) \cdot N(b) = 1$, so $N(a) = \pm 1$. Conversely, if $N(a) = \pm 1$, then $a \cdot (\pm \sigma(a)) = 1$, so a is a unit.

We observed

$$(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 2 \cdot 3.$$

All of these factors are irreducible in $\mathbb{Z}[\sqrt{10}]$. For example, if $2 = ab$, then $N(2) = N(ab)$, that is, $4 = N(a) \cdot N(b)$, so $N(a) \in \{\pm 1, \pm 2, \pm 4\}$. But $N(a)$ is a square *modulo* 10, so $N(a) \equiv 0, \pm 1, \pm 4, 5 \ (10)$. Therefore one of $N(a)$ or $N(b)$ is ± 1, so it is a unit.

* * * * *

If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$. But do we have the converse? We do if c is invertible (is a unit) *modulo* n. In that case, $cd \equiv 1 \pmod{n}$ for some d, and then

$$\begin{aligned} ac \equiv bc \pmod{n} &\implies acd \equiv bcd \pmod{n} \\ &\implies a \equiv b \pmod{n}. \end{aligned}$$

Invertibility of c *modulo* n is equivalent to solubility of $cx \equiv 1 \pmod{n}$, or equivalently

$$cx + ny = 1.$$

Thus c is invertible *modulo* n if and only if c and n are co-prime.

Alternatively, if $ac \equiv bc \pmod{n}$, and c and n are co-prime, then we can argue by Euclid's Lemma that, since $n \mid bc - ac$, that is, $n \mid (b-a)c$, we have $n \mid b - a$, that is, $a \equiv b \pmod{n}$.

Suppose we simply have $\gcd(c, n) = d$. Then $\gcd(c, n/d) = 1$. Hence

$$\begin{aligned} ac \equiv bc \bmod n &\implies ac \equiv bc \bmod \frac{n}{d} \\ &\implies a \equiv b \bmod \frac{n}{d}. \end{aligned}$$

Conversely,

$$\begin{aligned} a \equiv b \bmod \frac{n}{d} &\implies \frac{n}{d} \mid b - a \\ &\implies \frac{cn}{d} \mid bc - ac \\ &\implies n \mid bc - ac \\ &\implies ac \equiv bc \bmod n. \end{aligned}$$

In short,

$$ac \equiv bc \bmod n \iff a \equiv b \bmod \frac{n}{\gcd(c, n)}.$$

For example, $6x \equiv 6 \pmod{9} \iff x \equiv 1 \pmod{3}$.

A longer problem is to solve

$$70x \equiv 18 \pmod{134}. \tag{$*$}$$

This reduces to

$$35x \equiv 9 \pmod{67},$$

or $35x + 67y = 9$. So there is a solution if and only if $\gcd(35, 67) \mid 9$. To *find* the solutions, we should solve $35x + 67y = 1$, which we can do with the Euclidean Algorithm:

$$\begin{aligned} 67 &= 35 \cdot 1 + 32, \\ 35 &= 32 \cdot 1 + 3, \\ 32 &= 3 \cdot 10 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

so $\gcd(35, 67) = 1$. We now have

$$\begin{aligned} 32 &= 67 - 35, \\ 3 &= 35 - 32 = 35 - (67 - 35) = 35 \cdot 2 - 67, \\ 2 &= 32 - 3 \cdot 10 = 67 - 35 - (35 \cdot 2 - 67) \cdot 10 = 67 \cdot 11 - 35 \cdot 21, \\ 1 &= 3 - 2 = 35 \cdot 2 - 67 - 67 \cdot 11 + 35 \cdot 21 = 35 \cdot 23 - 67 \cdot 12. \end{aligned}$$

In particular, $35 \cdot 23 \equiv 1 \pmod{67}$, so $(*)$ is equivalent to

$$\begin{aligned} x &\equiv 23 \cdot 9 \quad (67) \\ &\equiv 207 \quad (67) \\ x &\equiv 6 \quad (67), \\ x &\equiv 6, 73 \quad (134). \end{aligned}$$

* * * * *

A puzzle from a recent newspaper [*Guardian Weekly*] is mathematically the same as one attributed [1, Prob. 4.4.8–9, p. 83] to Brahmagupta (7th century C.E.): A man dreams he runs up a flight of stairs. If he takes the stairs 2, 3, 4, 5, or 6 at time, then one stair is left before the top. If he takes them 7 at a time, then he reaches the top exactly. How many stairs are there?

If x is that number, then

$$\begin{aligned} x &\equiv 1 \quad (\text{mod } 2, 3, 4, 5, 6), \\ x &\equiv 0 \quad (\text{mod } 7). \end{aligned}$$

But $\operatorname{lcm}(2, 3, 4, 5, 6) = 60$, so $x = 60n + 1$, where $7 \mid 60n + 1$. We have this when $n = 5$, hence when $n = 12, 19, \dots$

The general problem is to solve systems

$$x \equiv a_0 \bmod n_0 \ \&\ x \equiv a_1 \bmod n_1 \ \&\ \cdots \ \&\ x \equiv a_k \bmod n_k. \tag{†}$$

Let's start with two congruences:

$$x \equiv a \bmod n \ \&\ x \equiv b \bmod m. \tag{‡}$$

A solution will take the form

$$\begin{aligned} x &= a + nu \\ &= mv + b. \end{aligned}$$

So we should like to make $a \equiv mv \ (n)$ and $nu \equiv b \ (m)$. We can do this if $\gcd(n, m) = 1$. Then we have $nr \equiv 1 \ (m)$ and $ms \equiv 1 \ (n)$ for some r and s, so that a solution to (‡) is

$$x = ams + bnr.$$

This solution is unique *modulo* $\operatorname{lcm}(n, m)$, which is nm since $\gcd(n, m) = 1$.

We can solve (†) similarly, under the assumption

$$\gcd(n_i, n_j) = 1$$

whenever $i < j \leqslant k$. We have

$$x = a_0 m_0 n_1 \cdots n_k + a_1 n_0 m_1 n_2 \cdots n_k + \cdots + a_k n_0 \cdots n_{k-1} m_k,$$

where the m_i are chosen so that

$$m_0 n_1 \cdots n_k \equiv 1 \quad (n_0),$$

and so forth; this is possible since

$$\gcd(n_0, n_1 \cdots n_k) = 1.$$

The solution is unique *modulo* $n_0 \cdots n_k$. This is the **Chinese Remainder Theorem.**

7. October 16, 2007 (Tuesday)

Of the 13 books of Euclid's *Elements,* VII, VIII and IX concern number-theory. The last proposition in these books is:

Theorem (Euclid, IX.36). *If* $1+2+4+\dots+2^n$ *is prime, then the product*

$$2^n \cdot (1+2+\dots+2^n)$$

is perfect.

A number is **perfect** if it is the sum of its positive proper divisors:

$$6 = 1+2+3,$$
$$28 = 1+2+4+7+14.$$

Proof of theorem. Let $M_{n+1} = 1+2+4+\dots+2^n = \sum_{k=0}^{n} 2^k = 2^{n+1}-1$. If M_{n+1} is prime, then the positive divisors of $2^n \cdot M_{n+1}$ are the divisors of 2^n, perhaps multiplied by M_{n+1}. So they are

$$1,\ 2,\ 4,\ \dots,\ 2^n,\ M_{n+1},\ 2\cdot M_{n+1},\ 4\cdot M_{n+1},\ \dots,\ 2^n\cdot M_{n+1}.$$

The sum of these is $(1+2+4+\dots+2^n)\cdot(1+M_{n+1})$, which is $M_{n+1}\cdot 2^{n+1}$. Subtracting $2^n \cdot M_{n+1}$ itself leaves the same. □

The number 2^n-1, denoted by M_n, is called a **Mersenne number;** if it is prime, it is a **Mersenne prime.** (Mersenne was a 17th-century mathematician.) We do not know whether there are infinitely many Mersenne primes. However, if M_n is prime, then so is n, since $2^a-1 \mid 2^{ab}-1$, because of the identity

$$x^m - y^m = (x-y)\cdot(x^{m-1}+x^{m-2}\cdot y + x^{m-3}\cdot y^2 + \dots + x\cdot y^{m-2} + y^{m-1}).$$

* * * * *

One method of factorizing n is to get a table of primes and test whether $p \mid n$ when $p \leqslant \sqrt{n}$.

Fermat's method is to solve

$$x^2 - y^2 = n,$$

since then $n = (x+y)(x-y)$. This method always works in principle, since

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

We may assume n is odd, so if $n = ab$, then $a \pm b$ are even.

For example, the first square greater than $2\,279$ is $2\,304$, or 48^2, and $2\,304 - 2\,279 = 25 = 5^2$, so

$$2\,279 = (48+5)(48-5) = 53\cdot 43.$$

We can generalize the method by solving

$$x^2 \equiv y^2 \pmod{n}.$$

If $x^2 - y^2 = mn$, then find $\gcd(x+y,n)$ and $\gcd(x-y,n)$.

* * * * *

Suppose $p \nmid a$, that is, $\gcd(p,a) = 1$. What is a^{p-1} *modulo* p? Consider a, $2a$, …, $(p-1)a$. These are all incongruent *modulo* p, since

$$ia \equiv ja \pmod{p} \implies i \equiv j \pmod{p}.$$

But 1, 2, …, $p-1$ are also incongruent. There are only $p-1$ numbers incongruent with each other and 0 *modulo* p; so the numbers a, $2a$, …, $(p-1)a$ are congruent respectively with 1, 2, …, $p-1$ in some order. Now multiply:

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Since $(p-1)!$ and p are co-prime, we conclude:

$$\gcd(a,p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}.$$

This is **Fermat's Little Theorem.** Equivalently,

$$a^p \equiv a \pmod{p}$$

for *all* a.

Hence $m \equiv n \pmod{p-1} a^m \equiv a^m \pmod{p}$. For example,

$$6^{58} \equiv 6^{48+10} \equiv (6^{16})^3 \cdot 6^{10} \equiv 6^{10} \pmod{17}.$$

Since $10 = 8+2$, we have $6^{10} = 6^8 \cdot 6^2$; but $6^2 \equiv 36 \equiv 2 \ (17)$, so $6^8 \equiv 2^4 \equiv 16 \equiv -1 \ (17)$, and hence

$$6^{58} \equiv -2 \pmod{17}.$$

If $a^n \not\equiv a \pmod{n}$, then n must not be prime. For example, what is 2^{133} *modulo* 133? We have $133 = 128 + 4 + 1 = 2^7 + 2^2 + 1$, so $2^{133} = 2^{2^7} \cdot 2^{2^2} \cdot 2$. Also,

$$\begin{aligned}
2^2 &= 4;\\
2^{2^2} &= 4^2 = 16;\\
2^{2^3} &= 16^2 = 256 \equiv 123 \equiv -10 \pmod{133};\\
2^{2^4} &\equiv (-10)^2 = 100 \equiv -33 \pmod{133};\\
2^{2^5} &\equiv (-33)^2 = 1089 \equiv 25 \pmod{133};\\
2^{2^6} &\equiv 25^2 = 625 \equiv -40 \pmod{133};\\
2^{2^7} &\equiv (-40)^2 = 1600 \equiv 4 \pmod{133}.
\end{aligned}$$

Therefore

$$2^{133} \equiv 4 \cdot 16 \cdot 2 \equiv -5 \pmod{133},$$

so 133 must not be prime. Indeed, $133 = 7 \cdot 19$.

The converse of the Fermat Theorem fails: It may be that $a^n \equiv a \pmod{n}$ for all a, although n is not prime. First, n is a **pseudo-prime** if n is not prime, but

$$2^n \equiv 2 \pmod{n}.$$

Then 341 is a pseudo-prime. Indeed, $341 = 11 \cdot 31$; but

$$\begin{aligned}
2^{11} &= 2048 = 31 \cdot 66 + 2 \equiv 2 \pmod{31},\\
2^31 &= (2^{10})^3 \cdot 2 \equiv 2 \pmod{11}.
\end{aligned}$$

Hence $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ by the following.

Lemma. *If $a^p \equiv a \ (q)$ and $a^q \equiv a \ (p)$, then $a^{pq} \equiv a \ (pq)$.*

Proof. Under the hypothesis, we have

$$\begin{aligned} a^{pq} &= (a^p)^q \equiv a^q \equiv a \pmod{q}, \\ a^{pq} &= (a^q)^p \equiv a^p \equiv a \pmod{p}, \end{aligned}$$

and hence $a^{pq} \equiv a \pmod{\operatorname{lcm}(p,q)}$; but $\operatorname{lcm}(p,q) = pq$. □

Again, we now have $2^{361} \equiv 2 \pmod{361}$, so 361 is pseudo-prime.

Theorem. *If n is a pseudo-prime, then so is $2^n - 1$.*

Proof. Since n factors non-trivially as ab, but $2^a - 1 \mid (2^a)^b - 1$, we have that 2^a is a non-trivial factor of $2^n - 1$. So $2^n - 1$ is not prime. We assume also $2^n \equiv 2 \pmod{n}$; say $2^n - 2 = kn$. Then

$$2^{2^n-1} - 2 = 2 \cdot (2^{2^n-2} - 1) = 2 \cdot (2^{kn} - 1),$$

which has the factor $2^n - 1$; so $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$. □

One can ask whether $3^n \equiv 3 \pmod{n}$, for example. But a number n is called an **absolute pseudo-prime** or a **Carmichael number** if

$$a^n \equiv a \pmod{n}$$

for all n. Then 561 is a Carmichael number. Indeed,

$$561 = 3 \cdot 11 \cdot 17;$$

and

$$\begin{aligned} 3 - 1 = 2 &\mid 560 = 561 - 1; \\ 11 - 1 = 10 &\mid 560; \\ 17 - 1 = 16 &\mid 560. \end{aligned}$$

Hence

$$\begin{aligned} 3 \nmid a &\implies a^2 \equiv 1 \pmod{3} \implies a^{560} \equiv 1 \pmod{3}; \\ 11 \nmid a &\implies a^{10} \equiv 1 \pmod{11} \implies a^{560} \equiv 1 \pmod{11}; \\ 17 \nmid a &\implies a^{17} \equiv 1 \pmod{17} \implies a^{560} \equiv 1 \pmod{17}. \end{aligned}$$

Hence $a^{561} \equiv a \pmod{3, 11, 17}$ for *all* a, so

$$a^{561} \equiv a \pmod{561}.$$

In general, if $n = p_0 \cdot p_1 \cdots p_k$, where $p_0 < p_1 < \cdots < p_k$, and $p_i - 1 \mid n - 1$ for each i, then the same argument shows that n is an absolute pseudo-prime.

It is necessary here that n have no square factor. Indeed, if $a^n \equiv a \pmod{n}$ for all a, but $m^2 \mid n$, then $m^n \equiv m \pmod{n}$, so

$$m^n \equiv m \pmod{m^2}.$$

But if $n > 1$, then $m^n \equiv 0 \pmod{m^2}$, so $m \equiv 0 \pmod{m^2}$, which is absurd unless $m = \pm 1$.

8. October 18, 2007 (Thursday)

Can we solve $(p-1)! \equiv x \pmod{p}$? The answer is certainly not 0.

Theorem. *Suppose $n > 1$. Then $(n-1)! \equiv -1 \pmod{n}$ if and only if n is prime.*

This is called 'Wilson's Theorem,' though Wilson did not prove it. It was supposedly [3] known to al-Haytham (964–1040). It gives a theoretical test for primality, though not a practical one.

Proof of theorem. One of the two directions should be easier; which one? Suppose n is not prime, so that $n = ab$, where $1 < a < n$. Then $a \leqslant n-1$, so $a \mid (n-1)!$, so $a \nmid (n-1)! + 1$, so $n \nmid (n-1)! + 1$.

Now suppose n is a prime p. Each number on the list $1, 2, 3, \dots, p-1$ has an inverse *modulo* p. Also, $x^2 \equiv 1 \pmod{p}$ has only the solutions ± 1, that is, 1 and $p-1$, since it requires $p \mid x \pm 1$. So the numbers on the list $2, 3, \dots, p-2$ have inverses different from themselves. Hence we can partition these numbers into pairs $\{a, b\}$, where $ab \equiv 1 \pmod{p}$. Therefore $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. □

For example,

$$\begin{aligned}
2 \cdot 4 &\equiv 1 \pmod{7},\\
3 \cdot 5 &\equiv 1 \pmod{7},\\
4 \cdot 2 &\equiv 1 \pmod{7},\\
5 \cdot 3 &\equiv 1 \pmod{7},\\
6 \cdot 6 &\equiv 1 \pmod{7};
\end{aligned}$$

so $6! = (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 6 \equiv -1 \pmod{7}$. How can one find the inverses, other than by trial? Take successive powers:

$$\begin{aligned}
2^2 &= 4,\\
2^3 &= 8 \equiv 1 \pmod{7};
\end{aligned}
\qquad
\begin{aligned}
3^2 &= 9 \equiv 2 \pmod{7},\\
3^3 &\equiv 2 \cdot 3 \equiv 6 \pmod{7},\\
3^4 &\equiv 6 \cdot 3 \equiv 4 \pmod{7},\\
3^5 &\equiv 4 \cdot 3 \equiv 5 \pmod{7},\\
3^6 &\equiv 5 \cdot 3 \equiv 1 \pmod{7}.
\end{aligned}$$

So the invertible numbers *modulo* 7 compose a multiplicative group generated by 3, and we have

$$3 \cdot 3^5 \equiv 3^2 \cdot 3^4 \equiv 1 \pmod{7}.$$

An application of Wilson's Theorem is the following.

Theorem. *Let p be an odd prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Suppose $a^2 \equiv -1 \pmod{p}$. By the Fermat Theorem,

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p},$$

so $(p-1)/2$ must be even: $4 \mid p-1$, so $p \equiv 1 \pmod{4}$.

Conversely, by Wilson's Theorem, we have

$$\begin{aligned}-1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1)\\ &\equiv 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \frac{p-1}{2} \cdot \frac{p+1}{2}\\ &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \frac{1-p}{2}\\ &\equiv (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2}\right)!\right)^2.\end{aligned}$$

So if $p \equiv 1 \pmod 4$, then $x^2 \equiv -1 \pmod p$ is solved by $((p-1)/2)!$. □

For example,

$$-1 \equiv 4! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \equiv 2^2 \pmod 5,$$

while, *modulo* 13, we have

$$-1 \equiv 12! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot 3 \cdot (-3) \cdot 4 \cdot (-4) \cdot 5 \cdot (-5) \cdot 6 \cdot (-6) \equiv (6!)^2 \quad (13).$$

9. October 25, 2007 (Thursday)

We work now with positive integers only. If n is one of them, we define

$$\sigma(n)$$

as the sum of the (positive) divisors of n. Hence n is *perfect* if and only if $\sigma(n) = 2n$. For the *number* of positive divisors of n, we write

$$\tau(n).$$

For example,

$$\begin{aligned}\tau(12) &= 1+2+3+4+6+12 = 28,\\ \sigma(12) &= 1+1+1+1+1+\ 1\ = 6.\end{aligned}$$

Indeed, $12 = 2^2 \cdot 3$, so the divisors of 12 are

$$\begin{gathered}2^0 \cdot 3^0,\\ 2^1 \cdot 3^0,\\ 2^2 \cdot 3^0,\\ 2^0 \cdot 3^1,\\ 2^1 \cdot 3^1,\\ 2^2 \cdot 3^1.\end{gathered}$$

So the factors of 12 are determined by a choice from $\{0,1,2\}$ for the exponent of 2, and from $\{0,1\}$ for the exponent of 3. Hence

$$\tau(12) = (2+1) \cdot (1+1).$$

Similarly, each factor of 12 itself has two factors: one from $\{1, 2, 4\}$, and the other from $\{1, 3\}$; so

$$\begin{aligned}\sigma(12) &= (1 + 2 + 4) \cdot (1 + 3) \\ &= (1 + 2 + 2^2) \cdot (1 + 3) \\ &= \frac{2^3 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1}.\end{aligned}$$

These ideas work in general:

Theorem. *If $n = {p_1}^{k(1)} \cdot {p_2}^{k(2)} \cdots {p_n}^{k(n)}$, where $p_1 < p_2 < \dots p_n$, then*

$$\begin{aligned}\tau(n) &= (k(1) + 1) \cdot (k(2) + 1) \cdots (k(n) + 1), \\ \sigma(n) &= (1 + p_1 + {p_1}^2 + \cdots + {p_1}^{k(1)}) \cdot (1 + p_2 + {p_2}^2 + \cdots + {p_2}^{k(2)}) \cdots \\ &= \frac{{p_1}^{k(1)+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{k(2)+1} - 1}{p_2 - 1} \cdots \frac{{p_n}^{k(n)+1} - 1}{p_n - 1}\end{aligned}$$

We can abbreviate the definitions of σ and τ as follows:

$$\sigma(n) = \sum_{d|n} d,$$
$$\tau(n) = \sum_{d|n} 1.$$

Implicitly here, d ranges over the *positive* divisors of n.

Is there a relation between $\sigma(n)$ and $\tau(n)$? We have

n	$\tau(n)$	$\sigma(n)$	$\prod_{d\|n} d$
1	1	1	1
2	2	3	2
3	2	4	3
4	3	7	$8 = 2^3 = 4^{3/2}$
5	2	6	5
6	4	12	$36 = 6^2$
7	2	8	7
8	4	15	$64 = 8^2$
9	3	13	$27 = 3^3 = 9^{3/2}$
10	4	18	$100 = 10^2$

It appears that

$$\prod_{d|n} d = n^{\tau(n)/2}.$$

We can prove it thus:

$$\Big(\prod_{d|n} d\Big)^2 = \Big(\prod_{d|n} d\Big) \cdot \Big(\prod_{d|n} d\Big) = \Big(\prod_{d|n} d\Big) \cdot \Big(\prod_{d|n} \frac{n}{d}\Big) = \prod_{d|n} n = n^{\tau(n)}.$$

10. October 30, 2007 (Tuesday)

Suppose $\gcd(n, m) = 1$. Then $n = {p_1}^{k(1)} \cdots {p_r}^{k(r)}$, and $m = {q_1}^{\ell(1)} \cdots {q_s}^{\ell(s)}$, where the p_i and q_j are all distinct primes. Hence the prime factorization of nm is

$${p_1}^{k(1)} \cdots {p_r}^{k(r)} \cdot {q_1}^{\ell(1)} \cdots {q_s}^{\ell(s)},$$

so we have

$$\begin{aligned}\sigma(nm) &= \frac{{p_1}^{k(1)+1} - 1}{p_1 - 1} \cdots \frac{{p_r}^{k(r)+1} - 1}{p_r - 1} \cdot \frac{{q_1}^{\ell(1)+1} - 1}{q_1 - 1} \cdots \frac{{q_s}^{k(s)+1} - 1}{q_s - 1} \\ &= \sigma(n) \cdot \sigma(m).\end{aligned}$$

Similarly, $\tau(nm) = \tau(n) \cdot \tau(m)$. We say then that σ and τ are *multiplicative;* in general, a function f on the positive integers is **multiplicative** if

$$f(nm) = f(n) \cdot f(m)$$

whenever n and m are co-prime. We do not require the identity to hold in general. For example,

$$\sigma(2 \cdot 2) = \sigma(4) = 1 + 2 + 4 = 7 \neq 9 = (1 + 2) \cdot (1 + 2) = \sigma(2) \cdot \sigma(2).$$

The identify function $n \mapsto n$ and the constant function $n \mapsto 1$ are multiplicative. Since $\sigma(n) = \sum_{d|n} d$ and $\tau(n) = \sum_{d|n} 1$, the multiplicativity of σ and τ is a consequence of the following.

Theorem. *If f is multiplicative, and F is given by*

$$F(n) = \sum_{d|n} f(d), \tag{$*$}$$

then F is multiplicative.

Before working out a formal proof, we can see why the theorem ought to be true from an example. Note first that, if f is multiplicative and *non-trivial,* so that $f(n) \neq 0$ for some n, then

$$0 \neq f(n) = f(n \cdot 1) = f(n) \cdot f(1),$$

so $f(1) = 1$. If also f and F are related by $(*)$, then

$$\begin{aligned}F(36) &= F(2^2 \cdot 3^2) \\ &= f(1) + f(2) + f(4) + f(3) + f(6) + f(12) + f(9) + f(18) + f(36) \\ &= \quad f(1) \cdot f(1) + f(2) \cdot f(1) + f(4) \cdot f(1) + \\ &\quad + f(1) \cdot f(3) + f(2) \cdot f(3) + f(4) \cdot f(3) + \\ &\quad + f(1) \cdot f(9) + f(2) \cdot f(9) + f(4) \cdot f(9) \\ &= (f(1) + f(2) + f(4)) \cdot (f(1) + f(3) + f(9)) \\ &= F(4) \cdot F(9).\end{aligned}$$

Proof of theorem. If $\gcd(m, n) = 1$, then every divisor of mn is uniquely of the form de, where $d \mid m$ and $e \mid n$. This is because every *prime* divisor of mn is uniquely a divisor of

m or n. Hence

$$\begin{aligned}
F(mn) &= \sum_{d \mid mn} f(d) \\
&= \sum_{d \mid m} \sum_{e \mid n} f(de) \\
&= \sum_{d \mid m} \sum_{e \mid n} f(d) \cdot f(e) \\
&= \sum_{d \mid m} f(d) \cdot \sum_{e \mid n} f(e) \\
&= \Bigl(\sum_{d \mid m} f(d)\Bigr) \cdot \sum_{e \mid n} f(e),
\end{aligned}$$

which is $F(m) \cdot F(n)$ by $(*)$. □

If F is defined from f as in $(*)$, can we recover f from F? For example, when f is $n \mapsto n$, so that F is σ, then

$$\begin{aligned}
\sigma(12) &= 1 + 2 + 3 + 4 + 6 + 12 \\
\sigma(6) &= 1 + 2 + 3 + 6 \\
\sigma(4) &= 1 + 2 + 4 \\
\sigma(3) &= 1 + 3 \\
\sigma(2) &= 1 + 2 \\
\sigma(1) &= 1
\end{aligned}$$

so that

$$12 = \sigma(12) - \sigma(6) - \sigma(4) + \sigma(2).$$

Why are some terms added, others subtracted? Why didn't we need $\sigma(3)$ or $\sigma(1)$? Note that $12/3 = 4 = 2^2$, a square.

We have also

$$\begin{aligned}
\sigma(30) &= 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 \\
\sigma(15) &= 1 + 3 + 5 + 15 \\
\sigma(10) &= 1 + 2 + 5 + 10 \\
\sigma(6) &= 1 + 2 + 3 + 6 \\
\sigma(5) &= 1 + 5 \\
\sigma(3) &= 1 + 3 \\
\sigma(2) &= 1 + 2 \\
\sigma(1) &= 1
\end{aligned}$$

so that

$$30 = \sigma(30) - \sigma(15) - \sigma(10) - \sigma(6) + \sigma(5) + \sigma(3) + \sigma(2) - \sigma(1).$$

Here we have $30/15 = 2$, $30/10 = 3$, and $30/6 = 5$: each of these numbers has one prime factor. But $30/5 = 2 \cdot 3$, $30/3 = 2 \cdot 5$, and $30/2 = 3 \cdot 5$; each number here has two prime factors.

The **Möbius function,** μ, is given by

$$\mu(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some prime } p; \\ (-1)^r, & \text{if } n = p_1 \cdots p_r, \text{ where } p_1 < \cdots < p_r. \end{cases}$$

In particular, $\mu(1) = 1$.

Theorem (Möbius Inversion Formula). *If f determines F by the rule $(*)$, then F determines f by the rule*

$$f(n) = \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) \cdot F(d). \qquad (\dagger)$$

Proof. We just start calculating:

$$\begin{aligned} \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) \cdot F(d) &= \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) \cdot \sum_{e \mid d} f(e) \\ &= \sum_{d \mid n} \sum_{e \mid d} \mu\Big(\frac{n}{d}\Big) \cdot f(e). \end{aligned}$$

For all factors d and e of n, we have

$$e \mid d \iff \frac{n}{d} \mid \frac{n}{e}.$$

Therefore

$$\begin{aligned} \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) \cdot F(d) &= \sum_{e \mid n} \sum_{c \mid (n/e)} \mu(c) \cdot f(e) \\ &= \sum_{e \mid n} f(e) \cdot \sum_{c \mid (n/e)} \mu(c). \end{aligned}$$

We want to obtain $f(n)$ from this. It will be enough if we can show that $\sum_{c \mid (n/e)} \mu(c)$ is 0 unless $e = n$, in which case the sum is 1. So it is enough to show

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{otherwise.} \end{cases} \qquad (\ddagger)$$

This is easy when $n = p^r$. Indeed, we have

$$\begin{aligned} \sum_{d \mid p^r} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) \\ &= \begin{cases} 1, & \text{if } r = 0; \\ 1 - 1, & \text{if } r \geqslant 1. \end{cases} \end{aligned}$$

But also, μ is multiplicative. Indeed, suppose $\gcd(m, n) = 1$. If $p^2 \mid mn$, then we may assume $p^2 \mid m$, so $\mu(mn) = 0 = \mu(m) = \mu(m) \cdot \mu(n)$. But if $m = p_1 \cdots p_r$, and $n = q_1 \cdots q_s$, where all factors are distinct primes, then $\mu(mn) = (-1)^{r+s} = (-1)^{\cdot}(-1)^2 = \mu(m) \cdot \mu(n)$. So μ is multiplicative. But then we have $(\ddagger)$. For, if $n \neq 1$, then n has a prime factor p, and $n = p^r \cdot a$ for some positive r, where $\gcd(a, p) = 1$. Then $\mu(n) = \mu(p^r) \cdot \mu(a) = 0$. So $(\ddagger)$ holds. This completes the proof of the theorem. □

* * * * *

The Chinese Remainder Theorem can be understood with a picture. Since $\gcd(5, 6) = 1$ for example, the Theorem gives us a solution to

$$\begin{cases} x \equiv a_1 \pmod 5, \\ x \equiv a_2 \pmod 6, \end{cases}$$

—a solution that is unique *modulo* 30. In theory, we can find this solution by filling out a table diagonally as follows:

	0	1	2	3	4	5
0	0					
1		1				
2			2			
3				3		
4					4	

, then

	0	1	2	3	4	5
0	0					5
1		1				
2			2			
3				3		
4					4	

,

then

	0	1	2	3	4	5
0	0					5
1	6	1				
2		7	2			
3			8	3		
4				9	4	

, then

	0	1	2	3	4	5
0	0				10	5
1	6	1				11
2		7	2			
3			8	3		
4				9	4	

,

and ultimately

	0	1	2	3	4	5
0	0	25	20	15	10	5
1	6	1	26	21	16	11
2	12	7	2	27	22	17
3	18	13	8	3	28	23
4	24	19	14	9	4	29

.

Hence, for example, a solution to $x \equiv 2 \pmod 5$ & $x \equiv 3 \pmod 6$ is 27 (in row 2, column 3).

Making such a table is not always practical. But the possibility of making such a table will enable us to establish a generalization of Fermat's Theorem. Fermat tells that, if $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod p.$$

Euler's Theorem will give us a certain function ϕ such that, if $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod n.$$

11. November 1, 2007 (Thursday)

We have defined

$$\mu(n) = (-1)^r,$$

if n is the product of r *distinct* primes; otherwise, $\mu(n) = 0$. In particular, $\mu(1) = (-1)^0 = 1$. We have shown that μ is multiplicative, that is,

$$\mu(mn) = \mu(m) \cdot \mu(n),$$

provided $\gcd(m, n) = 1$. We have shown (‡). From, this, we have established the Möbius Inversion Formula: if (∗), then (†).

Now we define a new multiplicative function, the **Euler phi-function:** $\phi(n)$ is the number of x such that $0 \leqslant x < n$ and x is prime to n. Then

(a) $\phi(1) = 1$;
(b) $\phi(p) = p - 1$;
(c) $\phi(p^r) = p^r - p^{r-1}$ when $r > 0$.

Indeed, suppose $\gcd(a,p^r)\neq 1$. Then $\gcd(a,p^r)=p^k$ for some positive k. In particular, $p\mid a$. Conversely, if $p\mid a$, then $p\mid\gcd(a,p^r)$, so $\gcd(a,p^r)\neq 1$. Therefore $\phi(p^r)$ is the number of integers x such that $0\leqslant x<p^r$ and $p\nmid x$; so

$$\phi(p^r)=p^r-\frac{p^r}{p}=p^r\cdot\Bigl(1-\frac{1}{p}\Bigr).$$

If we can show ϕ is multiplicative, and $n={p_1}^{k(1)}\cdots{p_r}^{k(r)}$, then

$$\begin{aligned}\phi(n)&=\phi({p_1}^{k(1)})\cdots\phi({p_r}^{k(r)})\\&={p_1}^{k(1)}\cdot\Bigl(1-\frac{1}{p_1}\Bigr)\cdots{p_r}^{k(r)}\cdot\Bigl(1-\frac{1}{p_r}\Bigr)\\&={p_1}^{k(1)}\cdots{p_r}^{k(r)}\cdot\Bigl(1-\frac{1}{p_1}\Bigr)\cdots\Bigl(1-\frac{1}{p_r}\Bigr)\\&=n\cdot\Bigl(1-\frac{1}{p_1}\Bigr)\cdots\Bigl(1-\frac{1}{p_r}\Bigr).\end{aligned}$$

But again, we must show ϕ is multiplicative. We do this with the Chinese Remainder Theorem.

Let us denote the set $\{x\in\mathbb{Z}\colon 0\leqslant x<n\}$ by $[0,n)$. Assume $\gcd(m,n)=1$. If $x\in[0,mn)$, then there is a unique a in $[0,m)$ such that $x\equiv a\pmod m$; likewise, there is a unique b in $[0,n)$ such that $x\equiv b\pmod n$. Thus we have a function $x\mapsto(a,b)$ from $[0,mn)$ into $[0,m)\times[0,n)$. Moreover, if x is prime to mn, then it is prime to m and to n, so a is prime to m, and b is prime to n.

Convsersely, by the Chinese Remainder Theorem, for every a in $[0,m)$ and b in $[0,n)$, there is a unique x in $[0,mn)$ such that

$$\begin{cases}x\equiv a\pmod{m},\\x\equiv b\pmod{n}.\end{cases}$$

Moreover, if a is prime to m, and b is prime to n, then x is prime to m and to n, hence to mn (that is, $\operatorname{lcm}(m,n)$). Therefore we have a bijection between the sets

$$\{x\in[0,mn)\colon\ \gcd(x,mn)=1\}$$

and

$$\{x\in[0,m)\colon\ \gcd(x,m)=1\}\times\{x\in[0,n)\colon\ \gcd(x,n)=1\}.$$

Therefore the sizes of these sets are equal; but by definition of ϕ, these sizes are $\phi(mn)$ and $\phi(m)\cdot\phi(n)$.

The idea can be seen in a table, as

	0	1	2	3	4	5	6
0	0	8	16	24	4	12	20
1	21	1	9	17	25	5	13
2	14	22	2	10	18	26	6
3	7	15	23	3	11	19	27

This gives the function $x\mapsto(a,b)$ from $[0,28)$ to $[0,4)\times[0,7)$. For example, 18 is in row 2 and column 4, so the function takes 18 to $(2,4)$. As 0 and 2 are not prime to 4, we delete rows 0 and 2; as 0 is not prime to 7, we delete column 0. The numbers remaining are prime to 28; and the *number* of these numbers—by definition, $\phi(28)$—is $2 \cdot 6$, which is $\phi(4) \cdot \phi(7)$.

	0	1	2	3	4	5	6
0							
1		1	9	17	25	5	13
2							
3		15	23	3	11	19	27

Burton [1] also uses a table of numbers, but written in the usual order:

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

The numbers prime to 7 are all in the first column, so delete it:

1	2	3	4	5	6
8	9	10	11	12	13
15	16	17	18	19	20
22	23	24	25	26	27

Then the number of remaining columns is $\phi(7)$. In each of these columns, just two numbers are prime to 4 (since each column contains a complete set of residues *modulo* 4). If we delete the numbers *not* prime to 4, what remains is the following:

1		3		5	
	9		11		13
15		17		19	
	23		25		27

Again, there are $\phi(4) \cdot \phi(7)$ numbers left, or $\phi(28)$.

12. November 6, 2007 (Tuesday)

We have defined

$$\phi(n) = |\{x \in \mathbb{Z} \colon 0 \leqslant x < n \ \&\ \gcd(x, n) = 1\}|.$$

To find a particular value, we can use a variant of the Sieve of Eratosthenes. For example, say we want $\phi(30)$. As $30 = 2 \cdot 3 \cdot 5$, we write down the numbers from 0 to 29 (or 1 to 30) and eliminate the multiples of 2, 3, or 5:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29

	1		3		5		7		9
	11		13		15		17		19
	21		23		25		27		29

	1				5		7		
	11		13				17		19
			23		25				29

	1						7		
	11		13				17		19
			23						29

As 8 numbers remain, we have $\phi(30) = 8$.

Our list of numbers had 10 columns and 3 rows. When we eliminated multiples of 2 and 5, we eliminated the columns headed by 0, 2, 4, 5, 6, and 8. The remaining columns were headed by 1, 3, 7, and 9: four numbers. Therefore $\phi(10) = 4$. In each of the remaining columns, the entries are incongruent *modulo* 3. Indeed, the numbers differ by 10 or 20, and these are not divisible by 3. So, in each column, exactly one entry is a multiple of 3. When it is eliminated, there are $4 \cdot 2$ entries remaining: this is $\phi(10) \cdot \phi(3)$. Thus, multiplicativity of ϕ is established. Alternatively, as last time, we can tabulate the numbers from 0 to 29 thus:

	0	1	2	3	4	5	6	7	8	9
0	0	21	12	3	24	15	6	27	18	9
1	10	1	22	13	4	25	16	7	28	19
2	20	11	2	23	14	5	26	17	8	29

Eliminating multiples of 2, 3, and 5 means eliminating certain columns *and* rows:

	0	1	2	3	4	5	6	7	8	9
0										
1		1		13				7		19
2		11		23				17		29

In general, we have

$$\begin{aligned} \phi(p) &= p - 1; \\ \phi(p^s) &= p^s - p^{s-1} = p \cdot \Bigl(1 - \frac{1}{p}\Bigr), && \text{if } s > 0; \\ \phi(mn) &= \phi(m) \cdot \phi(n), && \text{if } \gcd(m, n) = 1. \end{aligned}$$

Hence, if n has the distinct prime divisors $p_1, \dots, p_s$, then

$$\phi(n) = n \cdot \prod_{k=1}^{s} \Bigl(1 - \frac{1}{p_i}\Bigr).$$

We can write this more neatly as

$$\phi(n) = n \cdot \prod_{p \mid n} \Bigl(1 - \frac{1}{p}\Bigr).$$

For example,

$$\phi(30) = 30 \cdot \Bigl(1 - \frac{1}{2}\Bigr) \cdot \Bigl(1 - \frac{1}{3}\Bigr) \cdot \Bigl(1 - \frac{1}{5}\Bigr) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$$

Since 180 has the same prime divisors as 30, we have

$$\frac{\phi(180)}{\phi(30)} = \frac{180}{30} = 6,$$

so $\phi(180) = 6\phi(30) = 48$. But 15 and 30 do not have the same prime divisors, and we cannot expect $\phi(15)/\phi(30)$ to be $15/30$, or $1/2$; indeed, $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8 = \phi(30)$.

Theorem (Euler)**.** *If* $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Fermat's Theorem is the special case when $n = p$. But we do *not* generally have $a^{\phi(n)+1} \equiv a \pmod{n}$ for arbitrary a. For example, $\phi(12) = 4$, but $2^5 = 32 \equiv 8 \pmod{12}$; so

$$2^{\phi(12)+1} \not\equiv 2 \pmod{12}.$$

Proof of Euler's Theorem. Assume $\gcd(a, n) = 1$. We can write $\{x \in \mathbb{Z} \colon 0 \leqslant x < n \;\&\; \gcd(x, n) = 1\}$ as

$$\{b_1, b_2, \dots, b_{\phi(n)}\}.$$

Then we can obtain $a^{\phi(n)}$ from

$$\prod_{k=1}^{\phi(n)} (ab_k) = a^{\phi(n)} \cdot \prod_{k=1}^{\phi(n)} b_k.$$

As the two products are invertible *modulo* n, it is enough now to show that the two products are congruent *modulo* n. As a is invertible *modulo* n, there is a function f from $\{0, 1, \dots, \phi(n)\}$ to itself such that

$$ab_i \equiv b_{f(i)} \pmod{n}$$

for each i. Moreover, if $f(i) = f(j)$, then

$$ab_i \equiv b_{f(i)} \equiv b_{f(j)} \equiv ab_j \pmod{n},$$

so $b_i \equiv b_j \pmod{n}$, hence $i = j$. So f is a permutation. Therefore

$$\prod_{k=1}^{\phi(n)} b_k \equiv \prod_{k=1}^{\phi(n)} b_{f(k)} \equiv \prod_{k=1}^{\phi(n)} (ab_k) \pmod{n}.$$

As noted, the claim now follows. □

For example, to solve

$$369^{19587} x \equiv 1 \pmod{1000},$$

we compute

$$\phi(1000) = \phi(10^3) = \phi(2^3 \cdot 5^3) = \phi(2^3) \cdot \phi(5^3) = 4 \cdot 100 = 400.$$

Now reduce the exponent:

$$\frac{19587}{400} = 48 + \frac{387}{400}.$$

So we want to solve

$$\begin{aligned} 369^{387} x &\equiv 1 \pmod{1000}, \\ x &\equiv 369^{13} \pmod{1000}. \end{aligned}$$

Now proceed, using that $13 = 8+4+1 = 2^3+2^2+1$. Multiplication *modulo* 1000 requires only three columns:

$$\begin{array}{ccc} 3&6&9\\ 3&6&9\\ \hline 3&2&1\\ 1&4&\\ 7&&\\ \hline 1&6&1 \end{array} \quad \text{so } 369^2 \equiv 161 \quad (1000); \quad \begin{array}{ccc} 1&6&1\\ 1&6&1\\ \hline 1&6&1\\ 6&6&\\ 1&&\\ \hline 9&2&1 \end{array} \quad \text{so } 369^4 \equiv 161^2 \equiv 921 \quad (1000);$$

$$\begin{array}{ccc} 9&2&1\\ 9&2&1\\ \hline 9&2&1\\ 4&2&\\ 9&&\\ \hline 2&4&1 \end{array} \quad \text{so } 369^8 \equiv 921^2 \equiv 241 \quad (1000);$$

$$369^{13} \equiv 369^8 \cdot 369^4 \cdot 369 \equiv 241 \cdot 921 \cdot 369 \quad (1000);$$

$$\begin{array}{ccc} 2&4&1\\ 9&2&1\\ \hline 2&4&1\\ 8&2&\\ 9&&\\ \hline 9&6&1 \end{array} \qquad \begin{array}{ccc} 9&6&1\\ 3&6&9\\ \hline 6&4&9\\ 6&6&\\ 3&&\\ \hline 6&0&9 \end{array}$$

So the solution is $\boxed{x \equiv 609 \pmod{1000}.}$

* * * * *

Euler's Theorem gives a neat theoretical solution to Chinese-Remainder-Theorem problems: Suppose the integers $n_1, \dots, n_s$ are pairwise co-prime. Say we want to solve the system

$$\begin{cases} x \equiv a_1 \pmod{n_1}, \\ \dots \\ x \equiv a_s \pmod{n_s}. \end{cases}$$

Define

$$n = n_1 \cdots n_s;$$
$$N_i = \frac{n}{n_i}.$$

Then the system is solved by

$$x \equiv a_1 \cdot {N_1}^{\phi(n_1)} + \dots + a_s \cdot {N_s}^{\phi(n_s)}$$

Indeed, we have

$${N_i}^{\phi(n_i)} \equiv \begin{cases} 1 \pmod{n_i}; \\ 0 \pmod{n_j}, & \text{if } j \neq i. \end{cases}$$

* * * * *

As ϕ is multiplicative, so is

$$n \mapsto \sum_{d \mid n} \phi(d).$$

What *is* this function? The function is determined by its values at prime powers; so look at these. We have

$$\sum_{d|p^s} \phi(d) = \sum_{k=0}^{s} \phi(p^k) = 1 + \sum_{k=1}^{s} (p^k - p^{k-1}) =$$
$$= 1 + (p-1) + (p^2 - p) + \cdots + (p^s - p^{s-1}) = p^s.$$

Thus, the equation

$$\sum_{d|n} \phi(d) = n$$

holds when n is prime power. As both sides are *multiplicative* functions of n, the equation holds for all n. Thus we have

Theorem (Gauss). $\sum_{d|n} \phi(d) = n$ *for all positive integers* n.

For an alternative proof, partition the set $\{0, 1, \dots, n-1\}$ according to greatest common divisor with n. For example, suppose $n = 12$. We can construct a table as follows, where the rows are labelled with the divisors of 12. Each number x from 0 to 11 inclusive is assigned to row d, if $\gcd(x, 12) = d$.

	0	1	2	3	4	5	6	7	8	9	10	11
12	0											
6							6					
4					4				8			
3				3						9		
2			2								10	
1		1				5		7				11

But we have

$$0 \leqslant x < 12 \ \&\ \gcd(x, 12) = d \iff \gcd\Big(\frac{x}{d}, \frac{12}{d}\Big) = 1 \ \&\ 0 \leqslant \frac{x}{d} < \frac{12}{d}.$$

So the number of entries in row d is just $\phi(12/d)$. There are 12 entries in some row, so $12 = \sum_{d|12} \phi(d)$.

Is there anything noticeable about the table? Try $n = 20$:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
20	0																			
10											10									
5						5										15				
4					4				8				12				16			
2			2				6								14				18	
1		1		3				7		9		11		13				17		19

The entries are symmetric about a vertical axis, except for 0. Is there a theorem here? Define

$$S_n = \{x \in \mathbb{Z} \colon 0 \leqslant x < n \ \&\ \gcd(x, n) = 1\},$$

so $|S_n| = \phi(n)$. It appears that, when $n > 1$, then the average member of S_n is $n/2$:

$$\frac{\sum_{x \in S_n} x}{\phi(n)} = \frac{n}{2}.$$

Indeed, when $n > 1$, then S_n has the permutation $x \mapsto n - x$, so

$$2 \cdot \sum_{x \in S_n} x = \sum_{x \in S_n} x + \sum_{x \in S_n} (n - x) = \sum_{x \in S_n} (x + (n - x)) = \sum_{x \in S_n} x = n \cdot \phi(n).$$

Therefore

$$n > 1 \implies \sum_{x \in S_n} = \frac{n \cdot \phi(n)}{2}.$$

13. November 8, 2007 (Thursday)

Recall Gauss's Theorem:

$$\sum_{d \mid n} \phi(d) = n. \tag{$*$}$$

We gave two proofs; each one exhibits some useful techniques.

Let us make the tabular proof more precise. If $d \mid n$, let

$$S_d^n = \{x \colon 0 \leqslant x < n \ \&\ \gcd(x, n) = d\}.$$

Then $[0, n) = \bigcup_{d \mid n} S_d^n$, and the sets S_d^n are disjoint as d varies over the divisors of n. Therefore

$$n = |[0, n)| = \sum_{d \mid n} |S_d^n|. \tag{$\dagger$}$$

But we also have

$$\begin{aligned} x \in S_d^n &\iff 0 \leqslant x < n \ \&\ \gcd(x, n) = d \\ &\iff 0 \leqslant \frac{x}{d} < \frac{n}{d} \ \&\ \gcd\Big(\frac{x}{d}, \frac{n}{d}\Big) = 1 \\ &\iff \frac{x}{d} \in S_1^{n/d}. \end{aligned}$$

So we have a bijection $x \mapsto x/d$ from S_d^n to $S_1^{n/d}$, which means

$$|S_d^n| = |S_1^{n/d}|.$$

Also,

$$|S_1^{n/d}| = \phi\Big(\frac{n}{d}\Big).$$

So ($\dagger$) now becomes

$$n = \sum_{d \mid n} \phi\Big(\frac{n}{d}\Big) = \sum_{d \mid n} \phi(d).$$

The idea behind the last equation is frequently useful. For any function f (on the positive integers), we have

$$\sum_{d \mid n} f\Big(\frac{n}{d}\Big) = \sum_{d \mid n} f(d).$$

This is because the function $x \mapsto n/x$ is a permutation of the set of divisors of n.

Our other proof of Gauss's Theorem used the multiplicativeness of ($*$). It was enough to show that these are equal when n was a prime power. This technique is frequently useful.

* * * * *

To $(*)$ we can apply the Möbius Inversion Formula to get

$$\phi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot d = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \cdot \sum_{d|n} \frac{\mu(d)}{d}$$

and therefore

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

But we also have $\phi(n) = n \cdot \prod_{p|n}(1 - 1/p)$, so $\phi(n)/n = \prod_{p|n}(1 - 1/p)$. Therefore

$$\prod_{p|n}\Big(1 - \frac{1}{p}\Big) = \sum_{d|n} \frac{\mu(d)}{d}.$$

For example,

$$\sum_{d|12} \frac{\mu(d)}{d} = \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(6)}{6} + \frac{\mu(12)}{12} =$$

$$= 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6} = \Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big) = \prod_{p|12}\Big(1 - \frac{1}{p}\Big).$$

* * * * *

Recall Euler's Theorem:

$$\gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \pmod{n}.$$

This can be improved in some cases. For example, $255 = 3 \cdot 5 \cdot 17$, so $\phi(255) = \phi(3) \cdot \phi(5) \cdot \phi(17) = 2 \cdot 4 \cdot 16 = 128$, and hence

$$\gcd(a, 255) = 1 \implies a^{128} \equiv 1 \pmod{255}.$$

But by Fermat's Theorem,

$$\begin{aligned}
3 \nmid a &\implies a^2 \equiv 1 \pmod{3} \implies a^{16} \equiv 1 \pmod{3};\\
5 \nmid a &\implies a^4 \equiv 1 \pmod{5} \implies a^{16} \equiv 1 \pmod{5};\\
17 \nmid a &\implies a^{16} \equiv 1 \pmod{17}.
\end{aligned}$$

Therefore $\gcd(a, 255) = 1 \implies a^{16} \equiv 1 \pmod{3, 5, 17}$, that is,

$$\gcd(a, 255) = 1 \implies a^{16} \equiv 1 \pmod{255}.$$

In general, the **order** of a *modulo* n is the least positive k such that

$$a^k \equiv 1 \pmod{n}.$$

If such k does exist, then $a^k - 1 = n \cdot \ell$ for some ℓ, so

$$a \cdot a^{k-1} - n \cdot \ell = 1,$$

and therefore $\gcd(a, n) = 1$. Conversely, if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$, so a has an order *modulo* n.

Assuming $\gcd(a, n) = 1$, let us denote the order of a *modulo* n by

$$\mathrm{ord}_n(a).$$

For example, what is $\mathrm{ord}_{17}(2)$? Just compute powers of 2 *modulo* 17:

$$2,\ 4,\ 8,\ 16 \equiv -1,\ -2,\ -4,\ -8,\ -16 \equiv 1.$$

Then $\operatorname{ord}_{17}(2) = 8$. We also have

$$3,\ 9 \equiv -8,\ -24 \equiv -7,\ -21 \equiv -4,\ -12 \equiv 5,\ 15 \equiv -2,\ -6,\ -18 \equiv -1,$$
$$-3,\ 8,\ 7,\ 4,\ -5,\ 2,\ 6,\ 1.$$

Note how, halfway through, we just change signs. So $\operatorname{ord}_{17}(3) = 16$.

14. November 20, 2007 (Tuesday)

We have computed

k	1	2	3	4	5	6	7	8
$3^k \pmod{17}$	3	-8	-7	-4	5	-2	-6	-1

k	9	10	11	12	13	14	15	16
$3^k \pmod{17}$	-3	8	7	4	-5	2	6	1

Hence 16 is the least positive k such that $3^k \equiv 1 \pmod{17}$, so $\operatorname{ord}_{17}(3) = 16$. From the table we extract

k	1	2	3	4	5	6	7	8
$(-8)^k \pmod{17}$	-8	-4	-2	-1	8	4	2	1

which means $\operatorname{ord}_{17}(-8) = 8$. Likewise, $\operatorname{ord}_{17}(-4) = 4$, and $\operatorname{ord}_{17}(-1) = 2$. So we have

a	1	2	3	4	5	6	7	8
$\operatorname{ord}_{17}(a)$	1		16					
$\operatorname{ord}_{17}(-a)$	2			4				8

How can we complete the table? For example, what is $\operatorname{ord}_{17}(-7)$? Since $-7 \equiv 3^3 \pmod{17}$, and $\gcd(3, 16) = 1$, we have $\operatorname{ord}_{17}(-7) = 16$. Likewise, $\operatorname{ord}_{17}(5) = 16$. But $\operatorname{ord}_{17}(-2) = 16/\gcd(6, 16) = 8$, since $-2 \equiv 3^6 \pmod{17}$. This is by a general theorem to be proved presently. We complete the table thus:

a	1	2	3	4	5	6	7	8
$\operatorname{ord}_{17}(a)$	1	8	16	4	16	16	16	8
$\operatorname{ord}_{17}(-a)$	2	8	16	4	16	16	16	8

Theorem. *Suppose* $\gcd(a, n) = 1$. *Then*

(a) $a^k \equiv 1 \pmod{n}$ *if and only if* $\operatorname{ord}_n(a) \mid k$.
(b) $\operatorname{ord}_n(a^s) = \operatorname{ord}_n(a)/\gcd(s, \operatorname{ord}_n(a))$.
(c) $a^k \equiv a^\ell$ *if and only if* $k \equiv \ell \pmod{\operatorname{ord}_n(a)}$.

Proof. For (a), the reverse direction is easy. For the forward direction, suppose $a^k \equiv 1 \pmod{n}$. Now use division:

$$k = \operatorname{ord}_n(a) \cdot s + r$$

for some s and r, where $0 \leqslant r < \operatorname{ord}_n(a)$. Then

$$1 \equiv a^k \equiv a^{\operatorname{ord}_n(a)\cdot s + r} \equiv (a^{\operatorname{ord}_n(a)})^s \cdot a^r \equiv a^r \pmod{n}.$$

By minimality of $\operatorname{ord}_n(a)$ as an integer k such that $a^k \equiv 1 \pmod{n}$, we conclude $r = 0$. This means $\operatorname{ord}_n(a) \mid k$.

To prove (b), by (a) we have, *modulo* n,

$$(a^s)^k \equiv 1 \iff a^{sk} \equiv 1 \iff \operatorname{ord}_n(a) \mid sk \iff \frac{\operatorname{ord}_n(a)}{\gcd(s, \operatorname{ord}_n(a))} \mid k,$$

but also

$$(a^s)^k \equiv 1 \iff \mathrm{ord}_n(a^s) \mid k$$

Hence

$$\frac{\mathrm{ord}_n(a)}{\gcd(s, \mathrm{ord}_n(a))} \mid k \iff \mathrm{ord}_n(a^s) \mid k.$$

This is true for all k. Since orders are positive, we conclude

$$\frac{\mathrm{ord}_n(a)}{\gcd(s, \mathrm{ord}_n(a))} = \mathrm{ord}_n(a^s).$$

Finally, (c) follows from (a), since

$$\begin{aligned} a^k \equiv a^\ell \pmod{n} &\iff a^{k-\ell} \equiv 1 \pmod{n} \\ &\iff \mathrm{ord}_n(a) \mid k - \ell \\ &\iff k \equiv \ell \pmod{\mathrm{ord}_n(a)}. \end{aligned}$$

(We have used that $\gcd(a, n) = 1$, so that $a^{-\ell}$ exists.) □

Hence, from

k	1	2	3	4	5	6	7	8	9
$2^k \pmod{19}$	2	4	8	−3	−6	7	−5	9	−1
$2^{k+9} \pmod{19}$	−2	−4	−8	3	6	−7	5	−9	1

we obtain

a	1	2	3	4	5	6	7	8	9
$\mathrm{ord}_{19}(a)$	1	18	18	9	9	9	3	6	9
$\mathrm{ord}_{19}(-a)$	2	9	9	18	18	18	6	3	18

since

$$\begin{aligned} \mathrm{ord}_{19}(2^k) = 18 &\iff \gcd(k, 18) = 1 \\ &\iff k \equiv 1, 5, 7, 11, 13, 17 \pmod{18} \\ &\iff 2^k \equiv 2, -6, -5, -4, 3, -9 \pmod{19}; \\ \mathrm{ord}_{19}(2^k) = 9 &\iff \gcd(k, 18) = 2 \\ &\iff k \equiv 2, 4, 8, 10, 14, 16 \pmod{18} \\ &\iff 2^k \equiv 4, -3, 9, -2, 6, 5 \pmod{19}, \\ \mathrm{ord}_{19}(2^k) = 6 &\iff \gcd(k, 18) = 3 \\ &\iff k \equiv 3, 15 \pmod{18} \\ &\iff 2^k \equiv 8, -7 \pmod{19}, \\ \mathrm{ord}_{19}(2^k) = 3 &\iff \gcd(k, 18) = 6 \\ &\iff k \equiv 6, 12 \pmod{18} \\ &\iff 2^k \equiv 7, -8 \pmod{19}, \\ \mathrm{ord}_{19}(2^k) = 2 &\iff \gcd(k, 18) = 9 \\ &\iff k \equiv 9 \pmod{18} \\ &\iff 2^k \equiv -1 \pmod{19}. \end{aligned}$$

If $d \mid 19$, let $\psi(d)$ be the number of incongruent residues *modulo* 19 that have order d. Then we have

d	$\psi(d)$
18	6
9	6
6	2
3	2
2	1
1	1

Note that $\psi(d) = \phi(d)$ here.

*   *   *   *   *

We can understand what we are doing algebraically as follows. The set of congruence-classes *modulo* n is denoted by

$$\mathbb{Z}/(n)$$

or $\mathbb{Z}/n\mathbb{Z}$. On this set, addition and multiplication are well-defined: the set is a **ring.** The set of multiplicatively invertible elements of the ring is denoted by

$$(\mathbb{Z}/(n))^{\times}.$$

This set is closed under multiplication and inversion: it is a (multiplicative) **group.** Suppose $k \in (\mathbb{Z}/(n))^{\times}$. (More precisely one might write the element as $k + (n)$ or $\bar{k}$.) Then we have the function

$$x \mapsto k^x$$

from $\mathbb{Z}$ to $(\mathbb{Z}/(n))^{\times}$. Since $k^{x+y} = k^x \cdot k^y$, this function is a **homomorphism** from the additive group $\mathbb{Z}$ to the multiplicative group $(\mathbb{Z}/(n))^{\times}$.

We have shown that the function $x \mapsto 2^x$ is surjective onto $(\mathbb{Z}/(19))^{\times}$, and its kernel is (18). Hence (by the First Isomorphism Theorem for Groups), this function is an **isomorphism** from $\mathbb{Z}/(18)$ onto $(\mathbb{Z}/(19))^{\times}$:

$$\mathbb{Z}/(18) \cong (\mathbb{Z}/(19))^{\times},$$
$$(\{0,1,2,\dots,17\},+) \cong (\{1,2,3,\dots,18\},\ \cdot\ ).$$

*   *   *   *   *

If $\gcd(a,n) = 1$, and $\operatorname{ord}_n(a) = \phi(n)$, then a is called a **primitive root** of n. So we have shown that 3, but not 2, is a primitive root of 17, and 2 is a primitive root of 19. There is no formula for determining primitive roots: we just have to look for them. But once we know that 2 is a primitive root of 19, then we know that 2^5, 2^7, 2^{11}, 2^{13}, and 2^{17} are primitive roots—or rather, -6, -5, -4, 3, and -9 are primitive roots.

Theorem. *Every prime number has a primitive root.*

Proof. If $d \mid p-1$, let $\psi(d)$ be the number of incongruent residues *modulo* p that have order d. We shall show $\psi(p-1) \neq 0$. In fact, we shall show $\psi(d) = \phi(d)$.

Every number prime to p has an order *modulo* p, and this order divides $\phi(p)$, which is $p-1$; so

$$\sum_{d \mid p-1} \psi(d) = p-1.$$

By Gauss's Theorem we have $\sum_{d|p-1}\phi(d)=p-1$; therefore

$$\sum_{d|p-1}\psi(d)=\sum_{d|p-1}\phi(d). \tag{$*$}$$

Hence, to establish $\psi(d)=\phi(d)$, it is enough to show that $\psi(d)\leqslant\phi(d)$ whenever $d\mid p-1$. Indeed, if we show this, but $\psi(e)<\phi(e)$ for some divisor e of $p-1$, then

$$\sum_{d|p-1}\psi(d)=\sum_{\substack{d|p-1\\ d\neq e}}\psi(d)+\psi(e)<\sum_{\substack{d|p-1\\ d\neq e}}\phi(d)+\phi(e)=\sum_{d|p-1}\phi(d),$$

contradicting $(*)$.

If $\psi(d)=0$, then certainly $\psi(d)\leqslant\phi(d)$. So suppose $\psi(d)\neq 0$. Then $\operatorname{ord}_p(a)=d$ for some a. In particular, a is a solution of the congruence

$$x^n-1\equiv 0 \pmod{p}. \tag{$\dagger$}$$

But then every power of a is a solution, since $(a^k)^n=(a^n)^k$. Moreover, if $0<k<\ell\leqslant n$, then

$$a^k\not\equiv a^\ell \pmod{p}$$

by the earlier theorem. Hence the numbers a, a^2, ..., a^n are incongruent solutions to the congruence $(\dagger)$. Among these solutions, those that have order n *modulo* p are just those powers a^k such that $\gcd(k,n)=1$. The number of such powers is just $\phi(n)$.

Every number that has order n *modulo* p is a solution to $(\dagger)$. So we have that $\psi(d)=\phi(d)$ (under the assumption $\psi(d)>0$), *provided* we can show that *every* solution to $(\dagger)$ is on the list a, a^2, ..., a^n. But this is a consequence of the following theorem. □

15. November 22, 2007 (Thursday)

Theorem (Lagrange)**.** *Every congruence of the form*

$$x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n\equiv 0 \pmod{p}$$

*has n solutions or fewer (*modulo p*).*

Proof. Use induction. The claim is trivially true when $n=0$. Suppose it is true when $n=k$. Say the congruence

$$x^{k+1}+a_1x^k+\dots+a_kx+a_{k+1}\equiv 0 \pmod{p} \tag{$*$}$$

has a solution b. Then we can factorize the left member, and rewrite the congruence as

$$(x-a)\cdot(x^k+c_1x^{k-1}+\dots+c_{k-1}x+c_k)\equiv 0 \pmod{p}.$$

Any solution to this that is different from a is a solution of

$$x^k+c_1x^{k-1}+\dots+c_{k-1}x+c_k\equiv 0 \pmod{p}.$$

But by inductive hypothesis, there are at most k such solutions. Therefore $(*)$ has at most $k+1$ solutions. This completes the induction and the proof. □

How did we use that p is prime? We needed to know that, if $f(x)$ and $g(x)$ are polynomials, and $f(a)\cdot g(a)\equiv 0 \pmod{p}$, then either $f(a)\equiv 0 \pmod{p}$, or else $g(a)\equiv 0 \pmod{p}$. That is, if $mn\equiv 0 \pmod{p}$, then either $m\equiv 0 \pmod{p}$ or $n\equiv 0 \pmod{p}$. That is, if $p\mid mn$, then $p\mid m$ or $p\mid n$. This fails if p is replaced by a composite number.

From analysis, we have

$$\exp\colon\mathbb{R}\to\mathbb{R}^\times.$$

Here, $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$ (the multiplicatively invertible real numbers), and $\exp(x+y) = \exp(x)\cdot\exp(y)$. The range of exp is $(0,\infty)$, which is closed under multiplication and inversion. So exp is an isomorphism from $(\mathbb{R},+)$ onto $((0,\infty),\cdot\,)$. We have been looking at a similar isomorphism in discrete mathematics.

We have $|(\mathbb{Z}/(n))^\times| = \phi(n)$. A primitive root of n, if it exists, is a generator of the multiplicative group $(\mathbb{Z}/(n))^\times$. In particular:

(a) $(\mathbb{Z}/(2))^\times = \{1\}$, so 1 is a primitive root of 2.
(b) $(\mathbb{Z}/(3))^\times = \{1,2\}$, and $2^2 \equiv 1 \pmod 3$, so 2 is a primitive root of 3.
(c) $(\mathbb{Z}/(4))^\times = \{1,3\}$, and $3^2 \equiv 1 \pmod 4$, so 3 is a primitive root of 4.
(d) $(\mathbb{Z}/(5))^\times = \{1,2,3,4\}$, and $2^2 \equiv 4$, $2^3 \equiv 3$, and $2^4 \equiv 1 \pmod 5$, so 2 is a primitive root of 5.
(e) $(\mathbb{Z}/(6))^\times = \{1,5\}$, and $5^2 \equiv 1 \pmod 6$, so 5 is a primitive root of 6.
(f) $(\mathbb{Z}/(7))^\times = \{1,2,3,4,5,6\}$, and we have

k	1	2	3	4	5	6
2^k	2	4	1			
3^k	3	2	6	4	5	1

so 3 (but not 2) is a primitive root of 7.
(g) $(\mathbb{Z}/(8))^\times = \{1,3,5,7\}$, but $3^2 \equiv 1$, $5^2 \equiv 1$, and $7^2 \equiv 1 \pmod 8$, so 8 has no primitive root.

We have shown that primes have primitive roots, but the converse fails: not every number with a primitive root is prime. In fact, the following numbers have primitive roots:

(a) powers of odd primes;
(b) 2 and 4;
(c) doubles of powers of odd primes.

16. November 29, 2007 (Thursday)

Modulo 17, we have

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Reordering, we have

3^k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

If $3^k = \ell$, then we can denote k by $\log_3 \ell$. But we can think of these numbers as congruence-classes:

$$3^k \equiv \ell \pmod{17} \iff k \equiv \log_3 \ell \pmod{16}.$$

The usual properties hold:

$$\log_3(xy) \equiv \log_3 x + \log_3 y \pmod{16}; \qquad \log_3 x^n \equiv n \log_3 x \pmod{16}.$$

For example,

$$\log_3(11\cdot 14) \equiv \log_3 11 + \log_3 14 \equiv 7 + 9 \equiv 16 \equiv 0 \pmod{16},$$

and therefore $11 \cdot 17 \equiv 3^0 \equiv 1 \pmod{17}$.

In general, the base of logarithms will be a primitive root. If b is a primitive root of n, and $\gcd(a, n) = 1$, then there is some s such that

$$b^s \equiv a \pmod{n}.$$

Then s is unique *modulo* $\phi(n)$. Indeed, recall that

$$b^x \equiv b^y \pmod{n} \iff x \equiv y \pmod{\phi(n)}.$$

The least non-negative such s is defined to be $\log_b a$, *modulo* n.

Another application of logarithms, besides multiplication problems, is congruences of the form

$$x^d \equiv a \pmod{n}.$$

This is equivalent to

$$\begin{aligned} \log_b x^d &\equiv \log_b a \pmod{\phi(n)}, \\ d \log_b x &\equiv \log_b a \pmod{\phi(n)}. \end{aligned}$$

If this is to have a solution, then we must have

$$\gcd(d, \phi(n)) \mid \log_b a.$$

For example, let's work *modulo* 7:

k	0	1	2	3	4	5
3^k	1	3	2	6	4	5

ℓ	1	2	3	4	5	6
$\log_3 \ell$	0	2	1	4	5	3

Then we have, for example,

$$x^3 \equiv 2 \pmod{7} \iff 3 \log_3 x \equiv 2 \pmod{6},$$

so there is no solution, since $\gcd(3, 6) = 3$, and $3 \nmid 2$. But we also have

$$\begin{aligned} x^3 \equiv 6 \pmod{7} &\iff 3 \log_3 x \equiv 3 \pmod{6} \\ &\iff \log_3 x \equiv 1 \pmod{2} \\ &\iff \log_3 x \equiv 1, 3, 5 \pmod{6} \\ &\iff x \equiv 3^1, 3^3, 3^5 \pmod{7} \\ &\iff x \equiv 3, 6, 5 \pmod{7}. \end{aligned}$$

We expect no more than 3 solutions, by the Lagrange's Theorem. Is there an alternative to using logarithms? As $6 \equiv 3^3 \pmod{7}$, we have

$$x^3 \equiv 6 \pmod{7} \iff x^3 \equiv 3^3 \pmod{7};$$

but we cannot conclude from this $x \equiv 3 \pmod{7}$.

17. December 4, 2007 (Tuesday)

For congruences *modulo* 11, we can use the following table:

k	1	2	3	4	5	6	7	8	9	10	$\log_2 \ell \pmod{10}$
$2^k \pmod{11}$	2	4	-3	5	-1	-2	-4	3	-5	1	ℓ

We have then

$$\begin{aligned}
4x^{15} \equiv 7 \pmod{11} &\iff 4x^5 \equiv 7 \pmod{11}\\
&\iff \log_2(4x^5) \equiv \log_2 7 \pmod{10}\\
&\iff \log_2 4 + 5\log_2 x \equiv \log_2 7 \pmod{10}\\
&\iff 2 + 5\log_2 x \equiv 7 \pmod{10}\\
&\iff 5\log_2 x \equiv 5 \pmod{10}\\
&\iff \log_2 x \equiv 1 \pmod{2}\\
&\iff \log_2 x \equiv 1, 3, 5, 7, 9 \pmod{10}\\
&\iff x \equiv 2^1, 2^3, 2^5, 2^7, 2^9 \pmod{11}\\
&\iff x \equiv 2, 8, 10, 7, 6 \pmod{11}.
\end{aligned}$$

Why are there five solutions?

Theorem. *Suppose n has a primitive root r, so that logarithms with base r are defined. (So $a \equiv r^b \pmod{n}$ if and only if $\log_r a \equiv b \pmod{\phi(n)}$, when $\gcd(a, n) = 1$.) Assume $\gcd(a, n) = 1$. Let $d = \gcd(k, \phi(n))$. Then the following are equivalent:*

(a) *The congruence $x^k \equiv a \pmod{n}$ is soluble.*
(b) *The congruence has d solutions.*
(c) *$a^{\phi(n)/d} \equiv 1 \pmod{n}$.*

Proof. The following are equivalent:

$$\begin{gathered}
x^k \equiv a \pmod{n} \text{ is soluble;}\\
k \log x \equiv a \pmod{\phi(n)} \text{ if soluble;}\\
d \mid \log a;\\
\phi(n) \mid \frac{\phi(n)}{d} \cdot \log a;\\
\frac{\phi(n)}{d} \cdot \log a \equiv 0 \pmod{\phi(n)};\\
\log a^{\phi(n)/d} \equiv 0 \pmod{\phi(n)};\\
a^{\phi(n)/d} \equiv 1 \pmod{n}.
\end{gathered}$$

Thus (a) $\iff$ (c). Trivially, (b) $\implies$ (a). Finally, assume (a), so that $d \mid \log a$, as above. Then

$$\begin{aligned}
x^k \equiv a \pmod{n} &\iff k \log x \equiv \log a \pmod{\phi(n)}\\
&\iff \frac{k}{d} \cdot \log x \equiv \frac{\log a}{d} \pmod{\frac{\phi(n)}{d}}\\
&\iff \log x \equiv \frac{\log a}{k} \pmod{\frac{\phi(n)}{d}}\\
&\iff \log x \equiv \frac{\log a}{k} + \frac{\phi(n)}{d} \cdot j \pmod{\phi(n)},\\
&\qquad \text{where } j \in \{0, 1, \dots, d-1\}\\
&\iff x \equiv r^{(\log a)/k} \cdot (r^{\phi(n)/d})^j \pmod{n},\\
&\qquad \text{where } j \in \{0, 1, \dots, d-1\}.
\end{aligned}$$

These d solutions are incongruent, as $\operatorname{ord}_n(r) = \phi(n)$. □

* * * * *

We know that all primes have primitive roots. Now we show that the numbers with primitive roots are precisely:

$$2, 4, p^s, 2 \cdot p^s,$$

where p is an odd prime, and $s \geqslant 1$. We shall first show that the numbers *not* on this list do *not* have primitive roots:

Lemma. *If $k > 2$, then $2 \mid \phi(k)$.*

Proof. Suppose $k > 2$. Then either $k = 2^s$, where $s > 1$, or else $k = p^s \cdot m$ for some odd prime p, where $s > 0$ and $\gcd(p, m) = 1$. In the first case, $\phi(k) = 2^s - 2^{s-1} = 2^{s-1}$, which is even. In the second case, $\phi(k) = \phi(p^s) \cdot \phi(m)$, which is even, since $\phi(p^s) = p^s - p^{s-1}$, the difference of two odd numbers. □

Theorem. *If m and n are co-prime, both greater than 2, then mn has no primitive root.*

Proof. Suppose $\gcd(a, mn) = 1$. (This is the only possibility for a primitive root.) Then a is prime to m and n, so

$$a^{\phi(m)} \equiv 1 \pmod{m}; \qquad a^{\phi(n)} \equiv 1 \pmod{n};$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{m, n},$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{\operatorname{lcm}(m, n)},$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{mn}.$$

By the lemma, 2 divides both $\phi(m)$ and $\phi(n)$, so

$$\operatorname{lcm}(\phi(m), \phi(n)) \mid \frac{\phi(m)\phi(n)}{2},$$

that is, $\operatorname{lcm}(\phi(m), \phi(n)) \mid \phi(mn)/2$. Therefore

$$\operatorname{ord}_{mn}(a) \leqslant \frac{\phi(mn)}{2},$$

so a is not a primitive root of mn. □

Theorem. *If $k \geqslant 0$, then 2^{3+k} has no primitive root.*

Proof. Any primitive root of 2^{3+k} must be odd. Let a be odd. We shall show by induction that

$$a^{\phi(2^{3+k})/2} \equiv 1 \pmod{2^{3+k}}.$$

This means, since $\phi(2^{3+k}) = 2^{3+k} - 2^{2+k} = 2^{2+k}$, that we shall show

$$a^{2^{1+k}} \equiv 1 \pmod{2^{3+k}}.$$

The claim is true when $k = 0$, since $a^2 \equiv 1 \pmod{8}$ for all odd numbers a. Suppose the claim is true when $k = \ell$: that is,

$$a^{2^{1+\ell}} \equiv 1 \pmod{2^{3+\ell}}.$$

This means

$$a^{2^{1+\ell}} = 1 + 2^{3+\ell} \cdot m$$

for some m. Now square:

$$a^{2^{2+\ell}} = (a^{2^{1+\ell}})^2 = (1 + 2^{3+\ell} \cdot m)^2 = 1 + 2^{4+\ell} \cdot m + 2^{6+2\ell} \cdot m^2.$$

Hence $a^{2^{2+\ell}} \equiv 1 \pmod{2^{4+\ell}}$, that is,
$$a^{2^{1+(\ell+1)}} \equiv 1 \pmod{2^{3+(\ell+1)}};$$
so our claim is true when $k = \ell + 1$. This completes the induction and the proof. □

Now for the positive results. These will use the following.

Lemma. *Let r be a primitive root of p, and $k > 0$. Then*
$$\operatorname{ord}_{p^k}(r) = (p-1)p^\ell$$
for some ℓ, where $0 \leqslant \ell < k$.

Proof. Let $\operatorname{ord}_{p^k}(r) = n$. Then $n \mid \phi(p^k)$. But $\phi(p^k) = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$. Thus,
$$n \mid (p-1) \cdot p^{k-1}.$$
Also, $r^n \equiv 1 \pmod{p^k}$, so $r^n \equiv 1 \pmod{p}$, which means $\operatorname{ord}_p(r) \mid n$. But r is a primitive root of p, so $\operatorname{ord}_p(r) = \phi(p) = p - 1$. Therefore
$$p - 1 \mid n.$$
The claim now follows. □

Lemma. *p^2 has a primitive root. In fact, if r is a primitive root of p, then either r or $r + p$ is a primitive root of p^2.*

Proof. Let r be a primitive root of p. If r is a primitive root of p^2, then we are done. Suppose r is not a primitive root of p^2. Then $\operatorname{ord}_{p^2}(r) = p-1$, by the last lemma. Hence, *modulo* p^2, we have
$$\begin{aligned}(r+p)^{p-1} &\equiv r^{p-1} + (p-1) \cdot r^{p-2} \cdot p + \binom{p-1}{2} \cdot r^{p-3} \cdot p^2 + \cdots \\ &\equiv r^{p-1} + (p-1) \cdot r^{p-2} \cdot p \\ &\equiv 1 + (p-1) \cdot r^{p-2} \cdot p \\ &\equiv 1 - r^{p-2} \cdot p \\ &\not\equiv 1,\end{aligned}$$
since $p \nmid r$. (Note that this argument holds even if $p = 2$.) Hence $\operatorname{ord}_{p^2}(r+p) \neq p-1$, so by the lemma, the order must be $(p-1) \cdot p$, that is, $\phi(p^2)$. This means r is a primitive root of p^2. □

Theorem. *All odd prime powers (that is, all powers of odd primes) have primitive roots. In fact, a primitive root of p^2 is a primitive root of every power p^{2+k}.*

Proof. Assume p is an odd prime. We know p and p^2 have primitive roots. Let r be a primitive root of p^2. We prove by induction that r is a primitive root of p^{2+k}. The claim is trivially true when $k = 0$. Suppose it is true when $k = \ell$. This means
$$\operatorname{ord}_{p^{2+\ell}}(r) = (p-1) \cdot p^{1+\ell}.$$
In particular,
$$r^{(p-1) \cdot p^\ell} \not\equiv 1 \pmod{p^{2+\ell}}.$$
However, since $\phi(p^{1+\ell}) = (p-1) \cdot p^\ell$, we have
$$r^{(p-1) \cdot p^\ell} \equiv 1 \pmod{p^{1+\ell}}.$$

These two congruences imply that

$$r^{(p-1)\cdot p^\ell} = 1 + p^{1+\ell} \cdot m$$

for some m that is indivisible by p. Now raise both sides of this equation to the power p:

$$\begin{aligned} r^{(p-1)\cdot p^{\ell+1}} &= (r^{(p-1)\cdot p^\ell})^p \\ &= (1 + p^{1+\ell} \cdot m)^p \\ &= 1 + p \cdot p^{1+\ell} \cdot m + \binom{p}{2} \cdot (p^{1+\ell} \cdot m)^2 + \binom{p}{3} \cdot (p^{1+\ell} \cdot m)^3 + \cdots \\ &= 1 + p^{1+(\ell+1)} \cdot m + \binom{p}{2} \cdot p^{2+2\ell} \cdot m^2 + \binom{p}{3} \cdot p^{3+3\ell} \cdot m^3 + \cdots . \end{aligned}$$

Since $p > 2$, so that $p \mid \binom{p}{2}$, we have

$$\begin{aligned} r^{(p-1)\cdot p^{\ell+1}} &\equiv 1 + p^{1+(\ell+1)} \cdot m \pmod{p^{2+(\ell+1)}} \\ &\not\equiv 1 \pmod{p^{2+(\ell+1)}}. \end{aligned}$$

Therefore we must have

$$\operatorname{ord}_{p^{2+(\ell+1)}}(r) = (p-1) \cdot p^{1+(\ell+1)} = \phi(p^{2+(\ell+1)}),$$

which means r is a primitive root of $p^{2+(\ell+1)}$. □

It remains to show that $2 \cdot p^s$ also has a primitive root.

18. December 6, 2007 (Thursday)

If $\gcd(r, n) = 1$, then the following are equivalent:

(a) r is a primitive root of n;
(b) $\operatorname{ord}_n(r) = \phi(n)$;
(c) if $\gcd(a, n) = 1$, then $a \equiv r^b \pmod{n}$ for some b.

We have shown:

(a) Every prime p has a primitive root, r;
(b) either r or $r + p$ is a primitive root of p^2;
(c) if p is odd, then every primitive root of p^2 is a primitive root of p^{2+k}.

For example, 3 has the primitive root 2, since $2 \not\equiv 1 \pmod 3$, but $2^2 \equiv 1 \pmod 3$. Hence, either 2 or 5 is a primitive root of 9. In fact, both are. Using $5 \equiv -4 \pmod 9$, we have:

k	1	2	3	$6 = \phi(9)$
$2^k \pmod 9$	2	4	-1	1
$(-4)^k \pmod 9$	-4	-2	-1	1

Therefore 2 and -4 must be primitive roots of 27, and indeed

k	1	2	3	4	5	6	7	8	9	$18 = \phi(27)$
$2^k \pmod{27}$	2	4	8	-11	5	10	-7	13	-1	1
$(-4)^k \pmod{27}$	-4	-11	-10	13	2	-8	5	7	-1	1

But does 18 have a primitive root? We have

k	1	2	3	4	5	6	7
$(-4)^k$	-4	-2	8	4	2	-8	-4
5^k	5	7	-1	-5	-7	1	5

The powers of -4 and 5 cycle through six numbers in each case. Corresponding powers differ by 9: Since $-4 \equiv 5 \pmod 9$, we have $(-4)^k \equiv 5^k \pmod 9$. But the powers of -4 are not prime to 18, so -4 is not a primitive root of 18. However, 5 is.

Theorem. *If p is an odd prime, and r is a primitive root of p^s, then either r or $r+p^s$ is a primitive root of $2p^s$—whichever one is odd.*

Proof. Let r be an odd primitive root of p^s, so that $\gcd(r, 2p^s) = 1$. Let $n = \operatorname{ord}_{2p^s}(r)$. We want to show $n = \phi(2p^s)$. We have

$$n \mid \phi(2p^s).$$

Also $r^n \equiv 1 \pmod{2p^s}$, so $r^n \equiv 1 \pmod{p^s}$, and therefore

$$\operatorname{ord}_{p^s}(r) \mid n.$$

But $\operatorname{ord}_{p^s}(r) = \phi(p^s) = \phi(2p^s)$. Hence

$$\phi(2p^s) \mid n.$$

So $n = \phi(2p^s)$. □

* * * * *

Now we return to high-school-like problems. For example, how can we solve

$$x^2 - 4x - 1 \equiv 0 \pmod{11}?$$

Modulo 11, we have $x^2 - 4x - 1 \equiv x^2 - 4x - 12 \equiv (x-6)(x+2)$, so the solutions are 6 and -2, or rather 6 and 9. Alternatively, $x^2 - 4x - 1 \equiv x^2 + 7x + 10 \equiv (x+5)(x+2)$, so x is -5 or -2, that is, 6 or 9 again.

To solve

$$3x^2 - 4x - 6 \equiv 0 \pmod{13},$$

we can search for a factorization as before; but we can also **complete the square:**

$$\begin{aligned}
3x^2 - 4x - 6 \equiv 0 &\iff x^2 - \frac{4}{3}x - 2 \equiv 0 \\
&\iff x^2 - \frac{4}{3}x + \frac{4}{9} \equiv 2 + \frac{4}{9} \\
&\iff \left(x - \frac{2}{3}\right)^2 \equiv \frac{22}{9} \equiv 1 \\
&\iff x - \frac{2}{3} \equiv \pm 1 \\
&\iff x \equiv \frac{2}{3} \pm 1 \\
&\iff x \equiv \frac{5}{3} \text{ or } \frac{-1}{3} \\
&\iff x \equiv 6 \text{ or } 4.
\end{aligned}$$

Here we can divide by 3 because it is invertible *modulo* 13; indeed, $3 \cdot 9 \equiv 1 \pmod{13}$, so $1/3 \equiv 9 \pmod{13}$.

If we take this approach with the first problem, we have, *modulo* 11,

$$\begin{aligned}
x^2 - 4x - 1 \equiv 0 &\iff x^2 - 4x + 4 \equiv 5 \\
&\iff (x-2)^2 \equiv 5.
\end{aligned}$$

If 5 is a square *modulo* 11, then there is a solution; if not, not. But $5 \equiv 16 \equiv 4^2$, so we have

$$\begin{aligned} x^2 - 4x - 1 \equiv 0 &\iff (x-2)^2 \equiv 4^2 \\ &\iff x - 2 \equiv \pm 4 \\ &\iff x \equiv 2 \pm 4 \\ &\iff x \equiv 6 \text{ or } 9, \end{aligned}$$

as before. But the congruence

$$x^2 \equiv 5 \pmod{13}$$

has no solution. How do we know? One way is by trial. As 2 is a primitive root of 13, and 0 is not a solution of the congruence, every solution would be a power of 2. But we have, *modulo* 13,

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	-5	3	6	-1	-2	-4	5	-3	-6	1
2^{2k}	4	3	-1	-4	-3	1	4	3	-1	-4	-3	1

and 5 does not appear on the bottom row.

In general, if $p \nmid a$, we say a is a **quadratic residue** of p if the congruence

$$x^2 \equiv a \pmod{p}$$

is soluble; otherwise, a is a **quadratic non-residue** of p. So we have just seen that the quadratic residues of 13 are ± 1, ± 3, and ± 4, or rather 1, 3, 4, 9, 10, and 12; the quadratic non-residues are 2, 5, 6, 7, 8, and 11. So there are six residues, and six non-residues.

Theorem (Euler's Criterion)**.** *Let p be an odd prime, and* $\gcd(a, p) = 1$. *Then a is a quadratic residue of p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Proof. Let r be a primitive root of p. If $x^2 \equiv a \pmod{p}$ has a solution, then that solution is r^k for some k. Then

$$a^{(p-1)/2} \equiv ((r^k)^2)^{(p-1)/2} \equiv (r^k)^{p-1} \equiv 1 \pmod{p}$$

by Euler's Theorem.

In any case, $a \equiv r^\ell \pmod{p}$ for some ℓ. Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Then

$$1 \equiv (r^\ell)^{(p-1)/2} \equiv r^{\ell \cdot (p-1)/2} \pmod{p},$$

so $\operatorname{ord}_p(r) \mid \ell \cdot (p-1)/2$, that is,

$$p - 1 \mid \ell \cdot \frac{p-1}{2}.$$

Therefore $\ell/2$ is an integer, that is, ℓ is even. Say $\ell = 2m$. Then $a \equiv r^{2m} \equiv (r^m)^2 \pmod{p}$. □

19. December 11, 2007 (Tuesday)

Henceforth p is an odd prime, and $\gcd(a,p)=1$. We have defined quadratic residues and non-residues of p, and we have established Euler's Criterion: a is a quadratic residue of p if and only if $a^{(p-1)/2}\equiv 1 \pmod{p}$. What other congruence-class can $a^{(p-1)/2}$ belong to, besides 1? Only -1, since $a^{p-1}\equiv 1 \pmod{p}$, by Euler's Theorem. So $a^{(p-1)/2}\equiv -1 \pmod{p}$ if and only if a is a quadratic non-residue of p.

Another way to prove this is the following: Suppose a is a quadratic non-residue of p. If $b\in\{1,\dots,p-1\}$, then the congruence

$$bx\equiv a \pmod{p}$$

has a unique solution in $\{1,\dots,p-1\}$, and we may denote the solution by a/b. Then $b\neq a/b$, since a is not a quadratic residue of p. Now we define a sequence $(b_1,\dots,b_{p-1})$ recursively. If b_k has been chosen when $k<\ell<p-1$, then let b_ℓ be the least element of $\{1,\dots,p-1\}\smallsetminus\{b_1,a/b_1,\dots,b_{\ell-1},a/b_{\ell-1}\}$. We now have

$$\{1,\dots,p-1\}=\Bigl\{b_1,\frac{a}{b_1},\dots,b_{p-1},\frac{a}{b_{p-1}}\Bigr\}.$$

Now multiply everything together:

$$(p-1)!\equiv a^{(p-1)/2} \pmod{p}.$$

But we know $(p-1)!\equiv -1 \pmod{p}$ by Wilson's Theorem. Thus

$$a^{(p-1)/2}\equiv -1 \pmod{p}$$

when a is a quadratic non-residue of p.

Now suppose a is a quadratic residue of p. We choose the b_k as before, except this time let b_1 be the least positive solution of $x^2\equiv a \pmod{p}$, and replace a/b_1 with the next least positive solution, which is $p-b_1$. Multiplication now gives us

$$\begin{aligned}(p-1)! &\equiv b_1\cdot(p-b_1)\cdot b_2\cdot a/b_2\cdots b_{(p-1)/2}\cdot a/b_{(p-1)/2}\\ &\equiv -a\cdot a^{(p-1)/2-1}\\ &\equiv -a^{(p-1)/2} \pmod{p}.\end{aligned}$$

By Wilson's Theorem again, we have

$$a^{(p-1)/2}\equiv 1 \pmod{p}$$

when a is a quadratic residue of p.

* * * * *

Recall how division works in congruences (see p. 17: We have

$$ax\equiv ay \pmod{n} \implies x\equiv y \pmod{\frac{n}{\gcd(a,n)}}.$$

Indeed, let $d=\gcd(a,n)$. Then

$$\begin{aligned}ax\equiv ay \pmod{n} &\implies n\mid a(x-y)\\ &\implies \frac{n}{d}\mid\frac{a}{d}(x-y)\\ &\implies \frac{n}{d}\mid x-y\\ &\implies x\equiv y \pmod{\frac{n}{d}}.\end{aligned}$$

* * * * *

Again, p is an odd prime, and $p \nmid a$. We define the **Legendre symbol,** (a/p), by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p; \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

Then by Euler's Criterion we have immediately

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

We can now list the following properties of the Legendre symbol:

(a) $a \equiv b \pmod{p} \implies (a/p) = (b/p)$;
(b) $(a^2/p) = 1$;
(c) $(1/p) = 1$;
(d) $(-1/p) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}; \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

(We proved this equation, in effect, on p. 23.) Finally, we have

(e) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

since $(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}$, and equality of (ab/p) and $(a/p)(b/p)$ follows since each is ± 1 and $p > 2$. With these properties, we can calculate many Legendre symbols. For example,

$$\left(\frac{50}{19}\right) = \left(\frac{12}{19}\right) = \left(\frac{2}{19}\right)^2\left(\frac{3}{19}\right) = \left(\frac{3}{19}\right),$$

$$3^{(19-1)/2} \equiv 3^9 \equiv 3^8 \cdot 3 \equiv 9^4 \cdot 3 \equiv 81^2 \cdot 3 \equiv 5^2 \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv -1 \pmod{19},$$

so $(50/19) = -1$, which means the congruence $x^2 \equiv 50 \pmod{19}$ has no solution.

* * * * *

Theorem. *There are infinitely many primes p such that $p \equiv 3 \pmod{4}$.*

Proof. Suppose $(q_1, q_2, \ldots, q_n)$ is a list of primes. We shall prove that there is a prime p, not on this list, such that $p \equiv 3 \pmod{4}$. Let

$$s = 4q_1 \cdot q_2 \cdots q_n - 1.$$

Then $s \equiv 3 \pmod{4}$. Then s must have a prime factor p such that $p \equiv 3 \pmod{4}$. Indeed, if all prime factors of s are congruent to 1, then so must s be. But p is not any of the q_k. □

This argument fails when 3 is replaced by 1, since $3^2 \equiv 1 \pmod{4}$. Nonetheless, we still have:

Theorem. *There are infinitely many primes p such that $p \equiv 1 \pmod{4}$.*

Proof. Suppose $(q_1, q_2, \ldots, q_n)$ is a list of primes. We shall prove that there is a prime p, not on this list, such that $p \equiv 1 \pmod{4}$. Let

$$s = 2q_1 \cdot q_2 \cdots q_n.$$

Then $s^2 + 1$ is odd, so it is divisible by some odd prime p. Consequently, s is a solution of the congruence $x^2 \equiv -1 \pmod{p}$. This means $(-1/p) = 1$, so $p \equiv 1 \pmod{4}$, by (d) above. □

* * * * *

Theorem. $\displaystyle\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=0.$

Proof. Let r be a primitive root of p. Then

$$\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=\sum_{k=1}^{p-1}\left(\frac{r^k}{p}\right)=\sum_{k=1}^{p-1}\left(\frac{r}{p}\right)^k=\sum_{k=1}^{p-1}(-1)^k=0,$$

since $r^{(p-1)/2}\equiv -1 \pmod{p}$, since r is a primitive root. □

* * * * *

Lemma (Gauss). *Let p be an odd prime, and $\gcd(a,p)=1$. Then*

$$\left(\frac{a}{p}\right)=(-1)^n,$$

where n is the number of elements of the set

$$\{a,2a,3a,\dots,\frac{p-1}{2}a\}$$

whose remainders after division by p are greater than $p/2$.

For example, to find $(3/19)$, we can look at

$$3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27,$$

whose remainders on division by 19 are, respectively,

$$3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 2,\ 5,\ 8.$$

Of those, 12, 15, and 18 exceed $19/2$, and these are three; so

$$\left(\frac{3}{19}\right)=(-1)^3=-1.$$

Proof of Gauss's Lemma. If $1\leqslant k\leqslant p-1$, let b_k be such that

$$1\leqslant b_k\leqslant p-1,$$
$$ka\equiv b_k \pmod{p}.$$

Then $\{1,2,\dots,p-1\}=\{b_1,b_2,\dots,b_{p-1}\}$, because the b_k are distinct:

$$b_k=b_\ell \iff ka\equiv \ell a \iff k\equiv \ell.$$

In the set $\{b_1,b_2,\dots,b_{(p-1)/2}\}$, let n be the number of elements that are greater than $p/2$. We want to show

$$(-1)^n=\left(\frac{a}{p}\right).$$

There is some permutation σ of $\{1,2,\dots,(p-1)/2\}$ such that

$$b_{\sigma(1)}>b_{\sigma(2)}>\dots>b_{\sigma(n)}>\frac{p}{2}>b_{\sigma(n+1)}>\dots>b_{\sigma((p-1)/2)}.$$

Observe now that

$$b_{p-k}=p-b_k;$$

indeed, both numbers are in $\{1,2,\dots,p-1\}$, and

$$b_{p-k}\equiv (p-k)a\equiv -ka\equiv -b_k\equiv p-b_k \pmod{p}.$$

In particular, if $1 \leqslant k \leqslant (p-1)/2$, then $p - b_k \notin \{b_1, b_2, \dots, b_{(p-1)/2}\}$. Therefore

$$\{p - b_{\sigma(1)}, p - b_{\sigma(2)}, \dots, p - b_{\sigma(n)}, b_{\sigma(n+1)}, \dots b_{\sigma((p-1)/2)}\} = \left\{1, 2, \dots, \frac{p-1}{2}\right\}.$$

Now take products:

$$\begin{aligned}
\frac{p-1}{2}! &\equiv (p - b_{\sigma(1)})(p - b_{\sigma(2)}) \cdots (p - b_{\sigma(n)}) b_{\sigma(n+1)} \cdots b_{\sigma((p-1)/2)} \\
&\equiv (-1)^n \cdot b_{\sigma(1)} \cdots b_{\sigma((p-1)/2)} \\
&\equiv (-1)^n \cdot b_1 \cdots b_{(p-1)/2} \\
&\equiv (-1)^n \cdot a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a \\
&\equiv (-1)^n \cdot \frac{p-1}{2}! \cdot a^{(p-1)/2} \pmod{p}.
\end{aligned}$$

Therefore, since $p \nmid ((p-1)/2)!$, we have

$$1 \equiv (-1)^n \cdot a^{(p-1)/2} \equiv (-1)^n \cdot (a/p) \pmod{p}.$$

As both $(-1)^n$ and (a/p) are ± 1, the claim follows. □

We shall use Gauss's Lemma to prove the Law of Quadratic Reciprocity, by which we shall be able to relate (p/q) and (q/p) when both p and q are odd primes. Meanwhile, besides the direct application of Gauss's Lemma to computing Legendre symbols, we have:

Theorem. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. To apply Gauss's Lemma, we look at the numbers

$$2 \cdot 1,\ 2 \cdot 2,\ \dots,\ 2 \cdot \frac{p-1}{2}.$$

Each is its own remainder on division by p. Hence $(2/p) = (-1)^n$, where n is the number of integers k such that

$$\frac{p}{2} < 2k \leqslant p - 1,$$

or rather $p/4 < k \leqslant (p-1)/2$. This means

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right],$$

where $x \mapsto [x]$ is the greatest-integer function. Now consider the possibilities:

(a) $p = 8k + 1 \implies n = 4k - [2k + 1/4] = 2k$, even;
(b) $p = 8k + 3 \implies n = 4k + 1 - [2k + 3/4] = 2k + 1$, odd;
(c) $p = 8k + 5 \implies n = 4k + 2 - [2k + 5/4] = 4k + 1$, odd;
(d) $p = 8k + 7 \implies n = 4k + 3 - [2k + 7/4] = 4k + 2$, even.

In each case then, $(2/p)$ is as claimed. □

20. December 13, 2007 (Thursday)

As usual now, we assume p is an odd prime, and $p \nmid a$. Then the Legendre symbol (a/p) is in $\{1, -1\}$, and $(a/p) = 1$ if and only if $\exists x \in \mathbb{Z} : x^2 \equiv a \pmod{p}$. Rules that we have established include:

$$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right);$$

$$\left(\frac{a^2}{p}\right) = 1; \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right);$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}; \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

From these, we obtain the following table:

a	1	2	3	4	5	6	7	8	9	10	11	12
$(a/13)$	1		1	1					1	1		1

Indeed, under the squares 1, 4, and 9, we put 1. Also $4^2 = 16 \equiv 3$, so $(3/13) = 1$. Finally, $(-1)^{(13-1)/2} = (-1)^6 = 1$, so $(-1/13) = 1$, hence $(13 - a/13) = (-a/13) = (-1/13) \cdot (a/13) = (a/13)$; in particular, $(10/13) = 1$ and $(12/13) = 1$. So half of the slots have been filled with 1; the other half must get -1: In general, if r is a primitive root of p, then $(r/p) = -1$, and so $(r^k/p) = -1$ if and only if k is odd. So now we have

a	1	2	3	4	5	6	7	8	9	10	11	12
$(a/13)$	1	-1	1	1	-1	-1	-1	-1	1	1	1$-$	1

We proved Gauss's Lemma, and used it to show

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

As $13 \equiv -3 \pmod{8}$, we have $(2/13) = -1$, as we saw. We can also use this result about $(2/p)$ to find some primitive roots:

Theorem. *If p and $2p+1$ are both odd primes, then $2p+1$ has the primitive root $(-1)^{(p-1)/2} \cdot 2$, which is 2 if $p \equiv 1 \pmod{4}$, and is otherwise -2.*

Hence, for example, we have

p	3	5	11	23	29	41	53	83	89	113	131	173	179	191	233
$2p+1$	7	11	23	47	59	83	107	167	179	227	263	347	359	383	467
p.r. of $2p+1$	-2	2	-2	-2	2	2	2	-2	2	2	-2	2	-2	-2	2

Proof of theorem. Denote $2p+1$ by q. Then $\phi(q) = 2p$, whose divisors are 1, 2, p, and $2p$. Let $r = (-1)^{(p-1)/2} \cdot 2$. We want to show $\operatorname{ord}_q(r) \notin \{1, 2, p\}$. But $p \geqslant 3$, so $q \geqslant 7$, and hence $r^1, r^2 \not\equiv 1 \pmod{q}$. Hence $\operatorname{ord}_q(r) \notin \{1, 2\}$. It remains to show $\operatorname{ord}_q(r) \neq p$. But we know, from Euler's Criterion,

$$r^p \equiv r^{(q-1)/2} \equiv \left(\frac{r}{q}\right) \pmod{q}.$$

So it is enough to show $(r/q) = -1$. We consider two cases. If $p \equiv 1 \pmod{4}$, then $r = 2$, but also $q \equiv 3 \pmod{8}$, so $(r/q) = (2/q) = -1$. If $p \equiv 3 \pmod{4}$, then $r = -2$, but also $q \equiv 7 \pmod{8}$, and $(-1/q) = (-1)^{(q-1)/2} = (-1)^p = -1$, so $(r/q) = (-2/q) = (-1/q)(2/q) = -1$. $\square$

We now aim to establish the Law of Quadratic Reciprocity: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^n, \qquad \text{where} \qquad n=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Equivalently,

$$\left(\frac{q}{p}\right)=\begin{cases}(p/q), & \text{if } p\equiv 1 \text{ or } q\equiv 1 \pmod 4;\\ -(p/q), & \text{if } q\equiv 3\equiv p \pmod 4.\end{cases}$$

Then we shall be able to compute as follows:

$$\begin{aligned}
\left(\frac{365}{941}\right) &= \left(\frac{5}{941}\right)\left(\frac{73}{941}\right) && \text{[factorizing]}\\
&= \left(\frac{941}{5}\right)\left(\frac{941}{73}\right) && [5,73\equiv 1 \pmod{4}]\\
&= \left(\frac{1}{5}\right)\left(\frac{65}{73}\right) && \text{[dividing]}\\
&= \left(\frac{5}{73}\right)\left(\frac{13}{73}\right) && \text{[factorizing]}\\
&= \left(\frac{73}{5}\right)\left(\frac{73}{13}\right) && [5,13\equiv 1 \pmod{4}]\\
&= \left(\frac{3}{5}\right)\left(\frac{8}{13}\right) && \text{[dividing]}\\
&= \left(\frac{5}{3}\right)\left(\frac{2}{13}\right)^3 && [5\equiv 1 \pmod{4}\text{; factorizing}]\\
&= \left(\frac{2}{3}\right)\left(\frac{2}{13}\right) && [(p/q)^2=1]\\
&= (-1)(-1)=1 && [3\equiv 3 \pmod{8};\ 13\equiv -3 \pmod{8}].
\end{aligned}$$

To prove the Law, we shall use the following consequence of Gauss's Lemma:

Lemma. *If p is an odd prime, $p\nmid a$, and a is odd, then*

$$\left(\frac{a}{p}\right)=(-1)^n, \qquad \textit{where} \qquad n=\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right].$$

Proof. As in the proof of Gauss's Lemma, if $1\leqslant k\leqslant p-1$, we define b_k by

$$1\leqslant b_k\leqslant p-1 \qquad \& \qquad ka\equiv b_k \pmod{p}.$$

Then

$$ka=p\cdot\left[\frac{ka}{p}\right]+b_k,$$

so

$$\sum_{k=1}^{(p-1)/2}ka=p\cdot\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right]+\sum_{k=1}^{(p-1)/2}b_k. \tag{$*$}$$

For Gauss's Lemma, we introduced a permutation σ of $\{1,\dots,(p-1)/2\}$ such that, for some n,

$$b_{\sigma(1)}>\dots>b_{\sigma(n)}>\frac{p}{2}>b_{\sigma(n+1)}>\cdots b_{\sigma((p-1)/2)},$$

and we showed $(a/p)=(-1)^n$ after first showing

$$\left\{1,2,\dots,\frac{p-1}{2}\right\}=\{p-b_{\sigma(1)},\dots,p-b_{\sigma(n)},b_{\sigma(n+1)},\dots b_{\sigma((p-1)/2)}\}.$$

Now take sums:

$$\sum_{k=1}^{(p-1)/2}k=\sum_{k=1}^{n}(p-b_{\sigma(k)})+\sum_{\ell=n+1}^{(p-1)/2}b_{\sigma(\ell)}.$$

Subtracting this from $(*)$ (and using that $\sum_{k=1}^{(p-1)/2}b_{\sigma(k)}=\sum_{k=1}^{(p-1)/2}b_k$) gives

$$(a-1)\cdot\sum_{k=1}^{(p-1)/2}k=p\cdot\Big(\sum_{k=1}^{n}\left[\frac{ka}{p}\right]-n\Big)+2\cdot\sum_{k=1}^{n}b_{\sigma(k)}.$$

Since $a-1$ is even, but p is odd, we conclude

$$\sum_{k=1}^{n}\left[\frac{ka}{p}\right]\equiv n\pmod 2,$$

which yields the claim. □

21. December 18, 2007 (Tuesday)

A **Germain prime** (named for Sophie Germain, 1776–1831) is an odd prime p such that $2p+1$ is also prime. We showed that, if p is a Germain prime, then $2p+1$ has the primitive root $(-1)^{(p-1)/2}\cdot 2$. (However, it is not known whether there infinitely many Germain primes.) We used that

$$\left(\frac{2}{p}\right)=\begin{cases}1, & \text{if } p\equiv\pm1\pmod 8;\\ -1, & \text{if } p\equiv\pm3\pmod 8).\end{cases}$$

Another consequence of this formula is:

Theorem. *There are infinitely many primes congruent to* -1 modulo 8*.*

Proof. Let $q_1,\dots,q_n$ be a finite list of primes. We show that there is p not on the list such that $p\equiv-1\pmod 8$. Let

$$M=(4q_1\cdots q_n)^2-2.$$

Then $M\equiv-2\pmod{16}$, so M is not a power of 2; in particular, M has odd prime divisors. Also, for every odd prime divisor p of M, we have

$$(4q_1\cdots q_n)^2\equiv 2\pmod p,$$

so $(2/p)=1$, and therefore $p\equiv\pm1\pmod 8$. Since $M/2\equiv-1\pmod 8$, we conclude that not every odd prime divisor of M can be congruent to 1 *modulo* 8. □

Finally, for the proof of Quadratic Reciprocity, we showed that, if p is an odd prime, $p\nmid a$, and a is odd, then

$$\left(\frac{a}{p}\right)=(-1)^n,\qquad\text{where}\qquad n=\sum_{k=1}^{(p-1)/2}\left[\frac{ka}{p}\right].$$

Now we can establish:

Theorem (Law of Quadratic Reciprocity). *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^n, \qquad \text{where} \qquad n = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

This Law was:

- conjectured by Euler, 1783;
- imperfectly proved by Legendre, 1785, 1798;
- discovered and proved independently by Gauss, 1795, at age 18.

Proof of Quadratic Reciprocity (due to Gauss's student Eisenstein). By the lemma just mentioned,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^n, \qquad \text{where} \qquad n = \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2}\left[\frac{\ell q}{p}\right].$$

So it is enough to show

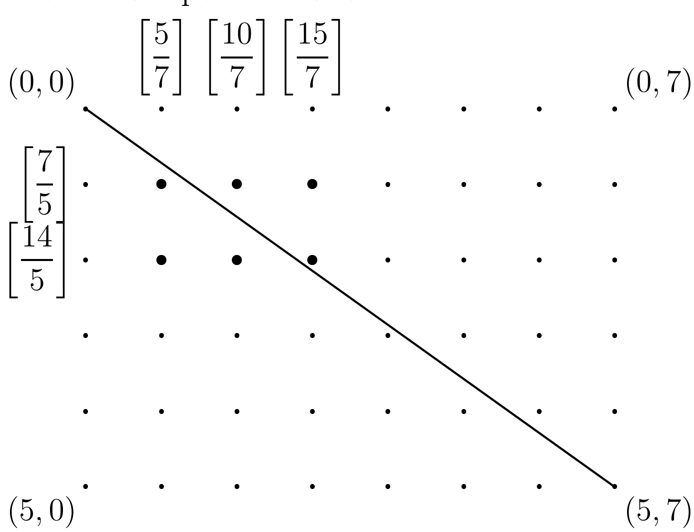
$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2}\left[\frac{\ell q}{p}\right].$$

First consider the example where $p = 5$ and $q = 7$. Then

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = 2\cdot 3 = 6;$$

$$\begin{aligned}\sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2}\left[\frac{\ell q}{p}\right] &= \left[\frac{5}{7}\right] + \left[\frac{10}{7}\right] + \left[\frac{15}{7}\right] + \left[\frac{7}{5}\right] + \left[\frac{14}{5}\right]\\ &= 0+1+2+1+2 = 6.\end{aligned}$$

Here 6 is the number of certain points in a lattice:



In general, $((p-1)/2)\cdot((q-1)/2)$ is the number of ordered pairs (ℓ, k) of integers such that

$$1 \leqslant \ell \leqslant \frac{p-1}{2}, \quad \& \quad 1 \leqslant k \leqslant \frac{q-1}{2}.$$

Then $\ell/k \neq p/q$, since p and q are co-prime. Hence the set of these pairs (ℓ, k) is a disjoint union $A \cup B$, where

$$\begin{aligned}(\ell,k)\in A &\iff \frac{\ell}{k}<\frac{p}{q};\\ (\ell,k)\in B &\iff \frac{\ell}{k}>\frac{p}{q} \iff \frac{k}{\ell}<\frac{q}{p}.\end{aligned}$$

Hence

$$\begin{aligned}A&=\left\{(\ell,k)\in\mathbb{Z}\times\mathbb{Z}\colon 1\leqslant k\leqslant\frac{q-1}{2}\ \&\ 1\leqslant\ell\leqslant\left[\frac{kp}{q}\right]\right\},\\ B&=\left\{(\ell,k)\in\mathbb{Z}\times\mathbb{Z}\colon 1\leqslant \ell\leqslant\frac{p-1}{2}\ \&\ 1\leqslant k\leqslant\left[\frac{\ell q}{p}\right]\right\},\end{aligned}$$

so

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=|A\cup B|=|A|+|B|=\sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right]+\sum_{\ell=1}^{(p-1)/2}\left[\frac{\ell q}{p}\right],$$

which is what we wanted to show. □

Again, the more useful form of the theorem is

$$\left(\frac{q}{p}\right)=\begin{cases}(p/q), & \text{if } p\equiv 1 \text{ or } q\equiv 1 \pmod 4;\\ -(p/q), & \text{if } q\equiv 3\equiv p \pmod 4.\end{cases}$$

Hence, for example,

$$\left(\frac{47}{199}\right)=-\left(\frac{199}{47}\right)=-\left(\frac{11}{47}\right)=\left(\frac{47}{11}\right)=\left(\frac{3}{11}\right)=-\left(\frac{11}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)=1.$$

We have used here the formula for $(2/p)$. What about $(3/p)$? We can compute:

$$\left(\frac{3}{p}\right)=\left\{\begin{array}{r}\left(\frac{p}{3}\right),\ \text{if } p\equiv 1 \pmod 4\\ -\left(\frac{p}{3}\right),\ \text{if } p\equiv 3 \pmod 4\end{array}\right\},\qquad \left(\frac{p}{3}\right)=\begin{cases}1, & \text{if } p\equiv 1 \pmod 3\\ -1, & \text{if } p\equiv 2 \pmod 3).\end{cases}$$

By the Chinese Remainder Theorem, we have

$$\begin{aligned}&\left\{\begin{matrix}p\equiv 1 & (4)\\ p\equiv 1 & (3)\end{matrix}\right\}\iff p\equiv 1 \quad (12), &&\left\{\begin{matrix}p\equiv 1 & (4)\\ p\equiv 2 & (3)\end{matrix}\right\}\iff p\equiv 5 \quad (12),\\ &\left\{\begin{matrix}p\equiv 3 & (4)\\ p\equiv 1 & (3)\end{matrix}\right\}\iff p\equiv 7 \quad (12), &&\left\{\begin{matrix}p\equiv 3 & (4)\\ p\equiv 2 & (3)\end{matrix}\right\}\iff p\equiv 11 \quad (12).\end{aligned}$$

Therefore

$$\left(\frac{3}{p}\right)=\begin{cases}1, & \text{if } p\equiv \pm 1 \pmod p,\\ -1, & \text{if } p\equiv \pm 5 \pmod p.\end{cases}$$

*   *   *   *   *

Assuming $\gcd(a,n)=1$, we know when the congruence $x^2\equiv a \pmod n$ has solutions, provided n is an odd prime; but what about the other cases? When $n=2$, then the congruence always has the solution 1. If $\gcd(m,n)=1$, and $\gcd(a,mn)=1$, then the congruence $x^2 \equiv a \pmod{mn}$ is soluble if and only if the system

$$\begin{cases} x^2 \equiv a \pmod{m}, \\ x^2 \equiv a \pmod{n} \end{cases}$$

is soluble. By the Chinese Remainder Theorem, the system is soluble if and only if the individual congruences are separately soluble. Indeed, suppose $b^2 \equiv a \pmod{m}$, and $c^2 \equiv a \pmod{n}$. By the Chinese Remainder Theorem, there is some d such that $d \equiv b \pmod{m}$ and $d \equiv c \pmod{n}$. Then $d^2 \equiv b^2 \equiv a \pmod{m}$, and $d^2 \equiv c^2 \equiv a \pmod{n}$, so $d^2 \equiv a \pmod{mn}$.

For example, suppose we want to solve

$$x^2 \equiv 365 \pmod{667}.$$

Factorize 667 as $23 \cdot 29$. Then we first want to solve

$$x^2 \equiv 365 \pmod{23} \quad \& \quad x^2 \equiv 365 \pmod{29}.$$

But we have $(365/23) = (20/23) = (5/23) = (23/5) = (3/5) = -1$ by the formula for $(3/p)$, so the first of the two congruences is insoluble, and therefore the original congruence is insoluble. It doesn't matter whether the second of the two congruences is insoluble.

Contrast with the following: $(2/11) = -1$, and $(7/11) = -(11/7) = -(4/7) = -1$; so the congruences

$$x^2 \equiv 2 \pmod{11}, \qquad x^2 \equiv 7 \pmod{11}$$

are insoluble; but $x^2 \equiv 14 \pmod{11}$ is soluble.

Now consider

$$x^2 \equiv 361 \pmod{667}.$$

One may notice that this has the solutions $x \equiv \pm 19$; but there are others, and we can find them as follows. We first solve

$$x^2 \equiv 16 \pmod{23}, \qquad x^2 \equiv 13 \pmod{29}.$$

The first of these is solved by $x \equiv \pm 4 \pmod{23}$ (and nothing else, since 23 is prime. For the second, note $13 \equiv 42, 71, 100 \pmod{29}$, so $x \equiv \pm 10 \pmod{29}$. So the solutions of the original congruence are the solutions of one of the following systems:

$$\left\{\begin{matrix} x \equiv 4 \pmod{23}, \\ x \equiv 10 \pmod{29} \end{matrix}\right\}, \qquad \left\{\begin{matrix} x \equiv 4 \pmod{23}, \\ x \equiv -10 \pmod{29} \end{matrix}\right\},$$

$$\left\{\begin{matrix} x \equiv -4 \pmod{23}, \\ x \equiv 10 \pmod{29} \end{matrix}\right\}, \qquad \left\{\begin{matrix} x \equiv -4 \pmod{23}, \\ x \equiv -10 \pmod{29} \end{matrix}\right\}.$$

One finds $x \equiv 19, 648, 280, 387 \pmod{667}$.

So now $x^2 \equiv a \pmod{n}$ is soluble if and only if the congruences

$$x^2 \equiv a \pmod{p^{k(p)}}$$

are soluble, where $n = \prod_{p|n} p^{k(p)}$. Assuming p is odd, and $(a/p) = 1$, we can show by induction that $x^2 \equiv a \pmod{p^k}$ is soluble for all positive k. Indeed, suppose $b^2 \equiv a \pmod{p^\ell}$, where $\ell \geqslant 1$. This means

$$b^2 = a + c \cdot p^\ell$$

for some c. Then

$$\begin{aligned}(b+p^\ell\cdot y)^2&=b^2+2bp^\ell\cdot y+p^{2\ell}\cdot y^2\\&=a+(c+2by)p^\ell+p^{2\ell}\cdot y^2\end{aligned}$$

Therefore $(b+p^\ell\cdot y)^2\equiv a \pmod{p^{\ell+1}} \iff c+2by\equiv 0 \pmod p$. But the latter congruence is soluble, since p is odd.

22. December 25, 2007 (Tuesday)

Assuming $\gcd(a,n)=1$, we have shown that $x^2\equiv a \pmod n$ is soluble if and only if $x^2\equiv a \pmod{p^{k(p)}}$ is soluble whenever $p\mid n$, where $n=\prod_{p\mid n}p^{k(p)}$. We also have that, if p is an odd prime, and $p\nmid a$, then the following are equivalent:

(a) $(a/p)=1$;
(b) $x^2\equiv a \pmod p$ is soluble;
(c) $x^2\equiv a \pmod{p^k}$ is soluble for some positive k;
(d) $x^2\equiv a \pmod{p^k}$ is soluble for all positive k.

We must finally consider powers of 2.

Theorem. *Suppose a is odd. Then:*

(a) $x^2\equiv a \pmod 2$ *is soluble;*
(b) $x^2\equiv a \pmod 4$ *is soluble if and only if* $a\equiv 1 \pmod 4$*;*
(c) *the following are equivalent:*
  (i) $x^2\equiv a \pmod 8$ *is soluble;*
  (ii) $x^2\equiv a \pmod{2^{2+k}}$ *is soluble for some positive* k*;*
  (iii) $x^2\equiv a \pmod{2^{2+k}}$ *is soluble for all positive* k*;*
  (iv) $a\equiv 1 \pmod 8$.

Proof. The first two parts are easy. So, are (ci)⇔(civ) and (ciii)⇒(cii)⇒(ci). We shall show (ci)⇒(ciii) by induction. Suppose $b^2\equiv a \pmod{2^{2+\ell}}$ for some positive ℓ. Then $b^2=a+2^{2+\ell}\cdot c$ for some c. Hence

$$\begin{aligned}(b+2^{1+\ell}\cdot y)^2&=b^2+2^{2+\ell}\cdot by+2^{2+2\ell}\cdot y^2\\&=a+2^{2+\ell}\cdot c+2^{2+\ell}\cdot by+2^{2+2\ell}\cdot y^2\\&=a+2^{2+\ell}\cdot(c+by)+2^{2+2\ell}\cdot y^2,\end{aligned}$$

and this is congruent to a *modulo* $p^{3+\ell}$ if and only if $c+by\equiv 0 \pmod 2$. But this congruence is soluble, since b is odd (since a is odd). □

* * * * *

A *Diophantine equation* is an equation for which the solutions sought are integers. We have considered such equations, as for example $ax+by=c$. Now we shall show that, if n is a natural number, then the Diophantine equation

$$x^2+y^2+z^2+w^2=n$$

is soluble.

If p is an odd prime, we know that the congruence $x^2\equiv -1 \pmod p$ is soluble if and only if $(-1/p)=1$, that is, $(-1)^{(p-1)/2}=1$, that is, $p\equiv 1 \pmod 4$.

Lemma. *For every prime p, the congruence*
$$x^2 + y^2 \equiv -1 \pmod p$$
is soluble.

Proof. The claim is easy when $p = 2$. So assume now p is odd. We define two sets:
$$A = \left\{x^2 \colon 0 \leqslant x \leqslant \frac{p-1}{2}\right\},$$
$$B = \left\{-y^2 - 1 \colon 0 \leqslant x \leqslant \frac{p-1}{2}\right\}.$$
We shall show that A and B have elements representing the same congruence-class *modulo* p; that is, A contains some a, and B contains some b, such that $a \equiv b \pmod p$. To prove this, note first that distinct elements of A are incongruent, and likewise of B. Indeed, if a_0 and a_1 are between 0 and $(p-1)/2$ inclusive, and ${a_0}^2 \equiv {a_1}^2 \pmod p$, then $a_0 \equiv \pm a_1 \pmod p$. If $a_0 \equiv -a_1$, then $a_0 = p - a_1$, which is absurd. Hence $a_0 \equiv a_1 \pmod p$, so $a_0 = a_1$.

Hence the elements of A represent $(p-1)/2 + 1$ distinct congruence-classes *modulo* p, and so do the elements of B. Since $2((p-1)/2+1) = p+1$, and there are only p distinct congruence-classes *modulo* p, there must be a class represented both in A and in B, by the Pigeonhole Principle. □

Another way to express the lemma is that, for all primes p, there are a, b, and m such that
$$a^2 + b^2 + 1 = mp.$$
Hence there are a, b, c, d, and m such that
$$a^2 + b^2 + c^2 + d^2 = mp.$$
We shall show that we can require $m = 1$. We can combine this with the following:

Theorem (Euler)**.** *The product of two sums of four squares is the sum of four squares.*

Proof. One can confirm that
$$\begin{aligned}(a^2+b^2+c^2+d^2)(q^2+r^2+s^2+t^2) = {} & (aq+br+cs+dt)^2 + \\ & (ar-bq+ct-ds)^2 + \\ & (as-bt-cq+dr)^2 + \\ & (at+bs-cr-dq)^2\end{aligned}$$
by expanding each side. □

Theorem (Lagrange)**.** *Every positive integer is the sum of four squares.*

Proof. By the lemma Euler's theorem, it is now enough to show the following. Let p be a prime. Suppose m is a positive integer such that
$$a^2 + b^2 + c^2 + d^2 = mp \tag{$*$}$$
for some a, b, c, and d. We shall show that the same is true for some smaller positive m, unless m is already 1.

First we show that, if m is even, then we can replace it with $m/2$. Indeed, if $a^2+b^2 = n$, then
$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{n}{2},$$

and if n is even, then so are $(a \pm b)/2$. In $(*)$ then, if m is even, then we may assume that $a^2 + b^2$ and $c^2 + d^2$ are both even, so

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{m}{2} \cdot p.$$

Henceforth we may assume m is odd. Then there are q, r, s and t *strictly* between $-m/2$ and $m/2$ such that

$$q \equiv a, \quad r \equiv b, \quad s \equiv c, \quad t \equiv d \pmod{m}.$$

Then

$$q^2 + r^2 + s^2 + t^2 \equiv 0 \pmod{m},$$

but also $q^2 + r^2 + s^2 + t^2 < m^2$, so

$$q^2 + r^2 + s^2 + t^2 = km$$

for some positive k less than m. We now have

$$(a^2 + b^2 + c^2 + d^2)(q^2 + r^2 + s^2 + t^2) = km^2 p.$$

By Euler's theorem, we know the left-hand side as a sum of four squares. Moreover, each of the squared numbers in that sum is divisible by m. Therefore we obtain kp as a sum of four squares. □

References

[1] David M. Burton. *Elementary Number Theory*. McGraw-Hill, Boston, sixth edition, 2007.

[2] Euclid. *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*. Dover Publications Inc., New York, 1956. Translated with introduction and commentary by Thomas L. Heath, 2nd ed.

[3] Graham Everest and Thomas Ward. *An introduction to number theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2005.

[4] D. A. Goldston, J. Pintz, and C. Y. Yıldırım. `http://arxiv.org`, 2005. arXiv:math/0508185v1 [math.NT].

[5] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. `http://arxiv.org`, 2004. arXiv:math/0404188v6 [math.NT].

[6] Nicomachus of Gerasa. *Introduction to Arithmetic*, volume XVI of *University of Michigan Studies, Humanistic Series*. University of Michigan Press, Ann Arbor, 1938. First printing, 1926.

[7] David Pierce. Foundations of number-theory. `http://www.math.metu.edu.tr/~dpierce/courses/365/`. 4 pp.

[8] Lucio Russo. *The forgotten revolution*. Springer-Verlag, Berlin, 2004. How science was born in 300 BC and why it had to be reborn, Translated from the 1996 Italian original by Silvio Levy.

Index

Mathematics Dept, Middle East Technical University, Ankara 06531, Turkey
E-mail address: dpierce@metu.edu.tr
URL: http://www.math.metu.edu.tr/~dpierce