Summary of MAT 221

David Pierce

January 2, 2013

dpierce@msgsu.edu.tr

http://mat.msgsu.edu.tr/~dpierce/Dersler/Number-theory/

Let $\mathbb{N} = \{1, 2, 3, \dots\} = \{x \in \mathbb{Z} \colon x > 0\}$. On $\mathbb{N}$ (or more generally on $\{n, n+1, n+2, \dots\}$), we can:

- define functions by **recursion** (so that, if A is some set, $c \in A$, and $f \colon A \to A$, then there is a unique function $k \mapsto a_k$ on $\mathbb{N}$ such that $a_1 = c$ and, for all k in $\mathbb{N}$, $a_{k+1} = f(a_k)$; if also $g \colon A \times \mathbb{N} \to A$, then there is a unique function $k \mapsto b_k$ on $\mathbb{N}$ such that $b_1 = c$ and, for all k in $\mathbb{N}$, $b_{k+1} = g(b_k, k)$);
- prove theorems by **induction;**
- prove theorems by **strong induction.**

For example, by strong induction, every natural number other than 1 has a prime factor: For, suppose $n \in \mathbb{N}$, and every element of $\{x \in \mathbb{N} \colon 1 < x < n\}$ has a prime factor. Either n is 1, or n is prime, or n has a factor k such that $1 < k < n$. In the last case, by the strong inductive hypothesis, k has a prime factor; but this factor is then a factor of n too.

We have the **Euclidean algorithm** for finding the greatest common divisor of two integers (not both of which are 0). If $\gcd(a, b) = d$, then we can also use the algorithm to solve

$$ax + by = d.$$

If $\gcd(a, n) = 1$, then $a \cdot a^{-1} \equiv 1 \pmod{n}$ for some number a^{-1}, which can be found by means of the Euclidean algorithm.

If $n \mid ab$ and $\gcd(n, a) = 1$, then $n \mid b$. In particular, if $p \mid ab$, but $p \nmid a$, then $p \mid b$. This can be used to prove the **Fundamental Theorem of Arithmetic.**

We can solve all **linear** congruences, that is, congruences of the form

$$ax \equiv b \pmod{n}.$$

By the **Chinese Remainder Theorem,** every linear system

$$x \equiv a_1 \pmod{n_1}, \qquad \dots, \qquad x \equiv a_k \pmod{n_k},$$

has a unique solution (which we can find) *modulo* $n_1 \cdots n_k$, assuming the moduli n_i are pairwise coprime. (What if they are not?)

An even number n is **perfect,** that is, $\sum_{d|n} = 2n$, if and only if

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

for some k such that $2^k - 1$ is prime.

If $n > 0$, we let

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}, \qquad \mathbb{Z}_n{}^{\times} = \{x \in \mathbb{Z}_n \colon \gcd(x, n) = 1\}.$$

Then by definition

$$\phi(n) = |\mathbb{Z}_n{}^{\times}|.$$

The values of ϕ (the **Euler phi-function**) can be found by two rules:

1. $\phi(ab) = \phi(a) \cdot \phi(b)$, if $\gcd(a, b) = 1$.
2. $\phi(p^{k+1}) = p^{k+1} - p^k = p^{k+1} \cdot (1 - 1/p)$.

Euler's Theorem is

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

(**Fermat's Theorem** is the special case when $n = p$.) The proof uses that if $\gcd(a, n) = 1$, then

$$\prod_{x \in \mathbb{Z}_n{}^{\times}} x \equiv \prod_{x \in \mathbb{Z}_n{}^{\times}} (ax) \equiv a^{\phi(n)} \cdot \prod_{x \in \mathbb{Z}_n{}^{\times}} x \pmod{n}.$$

Compare to the proof of **Wilson's Theorem:**

$$(p-1)! \equiv -1 \cdot 2 \cdot 2^{-1} \cdots \equiv -1 \pmod{p}.$$

We now have a method for computing powers *modulo* n, that is, for solving $a^k \equiv x \pmod{n}$. If $0 < k < \phi(n)$, we can find $b_1, \dots, b_m$ such that

$$0 \leqslant b_1 < \cdots < b_m, \qquad\qquad k = 2^{b_1} + \cdots + 2^{b_m};$$

and then a^k is easily computed as $a^{2^{b_1}} \cdots a^{2^{b_m}}$.

Henceforth p is an odd prime. With the usual quadratic formula, we can solve **quadratic** congruences

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

at least if we have a way to find square roots *modulo* p, when they exist. If the square root of d *modulo* p does exist, that is, if $x^2 \equiv d \pmod{p}$ is soluble, then d is called a **quadratic residue** of p.

If $\gcd(a, n) = 1$, then a has an **order** *modulo* n, namely the least positive exponent k such that $a^k \equiv 1 \pmod{n}$. We may denote this exponent by

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

Then $\operatorname{ord}_n(a) \mid \phi(n)$. For example, by the computations

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

we have $\operatorname{ord}_{17}(2) = 8$. Likewise, $\operatorname{ord}_{17}(3) = 16$, by the following.

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

In general, a is called a **primitive root** of n of $\operatorname{ord}_p(a) = \phi(n)$. For example, 3 is a primitive root of 17, but 2 is not. Also, 8 has no primitive root, since $\phi(8) = 4$, but $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. When they exist, primitive roots are found by trial; there is no formula for computing them.

Suppose a is a primitive root of p. Then

$$\operatorname{ord}_p(a^k) = \frac{p-1}{\gcd(k, p-1)}.$$

This gives us the following from the computations above:

k	0	14	1	12	5	15	11	10	(mod 16)
3^k	1	2	3	4	5	6	7	8	(mod 17)
$\operatorname{ord}_{17}(3^k)$	1	8	16	4	16	16	16	8	
$\gcd(k, 16)$	16	2	1	4	1	1	1	2	
$k+8$	8	6	9	4	13	7	3	2	(mod 16)
3^{k+8}	16	15	14	13	12	11	10	9	(mod 17)
$\operatorname{ord}_{17}(3^{k+8})$	2	8	16	4	16	16	16	8	
$\gcd(k+8, 16)$	8	2	1	4	1	1	1	2	

In general, if $\gcd(d, n) = 1$, let

$$\psi_n(d) = |\{x \in \mathbb{Z}_n{}^\times \colon \operatorname{ord}_n(x) = d\}|.$$

For example, from the last table we have the following.

d	1	2	4	8	16
$\psi_{17}(d)$	1	1	2	4	8
$\phi(d)$	1	1	2	4	8

In fact it is always true that[1]

$$\psi_p(d) = \phi(d).$$

In particular, since $\phi(p-1) \geqslant 1$, p must have a primitive root.[2]

If a is a primitive root of p, then the quadratic residues of p are the *even* powers of a (that is, the powers a^k such that k is even).

[1] The proof is that $\sum_{d|p-1} \phi(d) = p - 1 = \sum_{d|p-1} \psi_p(d)$ and $\psi_p(d) \leqslant \phi(d)$; but we have not seen all of the details.

[2] Only 2, 4, p^k, and $2p^k$ have primitive roots.