LECTURE NOTES AND FINAL REVIEW
May 18, 2012

JOHN WANG

1. Introduction and Mathematical Tools

Theorem 1.1. *Given $a, b \in \mathrm{Z}$ such that $a > 0$, $\exists q, r \in \mathrm{Z}$ such that $b = aq + r$ and $r < a$.*

Proof. Examine the set $S = \{b - ka : b - ka > 0, a > 0, a, r \in \mathrm{Z}\}$. We shall show that this set is nonempty (and it is clearly a subset of N). We know that $b - 0\dot{a} \in S$ so if $b > 0$, then the set is nonempty. If $b < 0$, then there exists a k such that $b - ka > 0$, which shows the set is nonempty. Thus, we can use the well-ordering principle so that there exists some r which is a minimum in the set S.

Now we shall show that $r < a$. Suppose not and $r \geq a$. Then we know that $r = b - ka \geq a$. Hwoever, we know that $b - (k+1)a \geq 0$ which means there is a smaller element in S, contradicting the minimality of r. □

Theorem 1.2. *Let $g = gcd(a, b)$. Then $\exists x_0, y_0 \in \mathrm{Z}$ such that $ax_0 + by_0 = g$.*

Proof. Let $S = \{ax + by : x, y \in \mathrm{Z}, ax + by > 0\}$. We know that the set is nonempty because you can choose $x, y = 1$ so that $a + b \in S$. Therefore, we can use the well ordering property to obtain a minimum g of S. We'll show that $g|a$ and $g|b$, and if there is any other divisor d of a and b, then $d|g$.

Assume that $g \nmid a$. Then there exists an $r > 0$ such that $a = gq + r$ where $r < g$. This means that $g = ax + by = (gq + r)x + by$. This means that $r = a(q - xq) - byq$. This shows that $r \in S$, which is a contradiction because $r < g$ which contradicts the minimality of g. We see that $g|b$ follows similarly.

Now assume that $d|a$ and $d|b$, then $d|ax + by = g$ as well by the properties of division. □

Construction 1.3. Euclidean Algorithm: Given two integers a, b:

(1) If a or b is negative, replace it by its negative.
(2) If $a > b$, switch a, b so that $a \leq b$.
(3) If $a = 0$, return b.
(4) Since $b \geq a$, write $b = aq + r$ where $0 \leq r < a$ and replace (a, b) with (r, a), and loop on 3.

Theorem 1.4. *Fundamental Theorem of Arithmetic: Any positive integer can be written as a product of primes uniquely.*

Proof. Existence. We will use induction to show existence, and suppose that that all integers less than or equal to n can be written as a product of primes. If $n + 1$ is a prime, then we are done because it can be written as $(1)(n + 1)$. If $n + 1$ is not a prime, then it is composite and can be decomposed into integers $k, q \leq n$ such that $kq = n$. Since k and q can be written as a product of primes, we can write $n + 1$ as a product of primes as well. This completes the induction step.

Uniqueness. Suppose there are two ways to write n as a product of primes: $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$.

Lemma 1.5. *If p is a prime and $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose $p \nmid a$, then we know that $gcd(p, a) = 1$ because p is a prime. We see that $p|ab$ which implies that $p|b$. □

Therefore, we see that $p_1|q_i$ for some $i \in \{1, 2, \dots, s\}$. However, since both p_1 and q_i are primes, we see that $p_1 = q_i$. This means that we can cancel p_1 and q_i, and obtain $p_2 \dots p_r = q_1 \dots q_{i-1} q_{i+1} \dots q_s$. Continuing downwards, we find that this happens for all the primes on the list, so that $p_1 \dots p_r$ is just a reordering of $q_1 \dots q_s$. □

Theorem 1.6. *Euclids Infinitude of Primes: There exist an infinite number of primes.*

Proof. Suppose by contradiction that this is not true. Then we can enumerate the primes $S = \{p_1, p_2, \dots, p_n\}$. Then we can construct the number $N = p_1 p_2 \dots p_n + 1$. We know that $p_i \nmid N$ for all $i \in \{1, \dots, n\}$ because $gcd(p_i, N) = 1$. This implies that no prime divides N. Moreover, N cannot be a prime because it is not listed in the set S. This means that it must be composite, and hence, it can be decomposed into a product of primes. However, we see no primes in S can be factors of N. This is a contradiction. □

Theorem 1.7. *$p^e || n!$ where $e = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots$.*

Proof. Consider the set $S = \{1, 2, \ldots, n\}$ which is the complete residue system modulo n. We know that $n! = n(n-1)(n-2)\ldots 1$. Moreover, we know that $\lfloor \frac{n}{p} \rfloor$ is the number of multiples of p in the set S. Likewise, $\lfloor \frac{n}{p^2} \rfloor$ is the number of multiples of p^2 in the set S. Thus, we see that $e = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \ldots$ is the total number of multiples of p in the set S. This means that p^e divides evenly into the product of S so that $p^e || n!$. □

2. Congruences

Lemma 2.1. *If $r_1, r_2, \ldots, r_k$ is a reduced residue system modulo m and $gcd(a, m) = 1$, then so is $ar_1, ar_2, \ldots, ar_k$.*

Proof. We need to show that $gcd(ar_1, m) = 1$. This is true because $gcd(a, m) = 1$ by assumption and $gcd(r_i, m) = 1$ by the definition of a reduced residue system. This implies that $gcd(ar_i, m) = 1$. Now we need to show that all ar_i are distinct modulo m. Suppose not. Then $ar_i \equiv ar_j \pmod{m}$ for some $i \neq j$. Then we see that $a(r_i - r_j) \equiv 0 \pmod{m}$. Since $gcd(a, m) = 1$, we know that $m \nmid a$ so that $m | r_i - r_j$. This implies that $r_i \equiv r_j \pmod{m}$ which is a contradiction. □

Theorem 2.2. *If $gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. We will prove this by invoking the lemma from above. Let $r_1, r_2, \ldots, r_k$ be a reduced residue system modulo m. Then we see that $ar_1 ar_2 \ldots ar_k \equiv r_1 r_2 \ldots r_k \pmod{m}$. This shows that $a^k \equiv 1 \pmod{m}$. Since $k = \phi(m)$ is the number of objects in the reduced residue system, we are finished with our theorem. □

Corollary 2.3. *Fermat's Little Theorem: If $gcd(a, m) = 1$, then $a^p \equiv a \pmod{p}$.*

Lemma 2.4. *The congruence $x^2 \equiv 1 \pmod{p}$ has only solutions $x \equiv \pm 1 \pmod{p}$.*

Proof. It is clear that $x^2 - 1 \equiv 0 \pmod{p}$ is another way to write the above equation. Factoring out the left side, we see that $(x-1)(x+1) \equiv 0 \pmod{p}$. This means that $p | (x-1)(x+1)$. Moreover, since $p \geq 2$, we know that $p | x - 1$ or $p | x + 1$. Thus, the only solutions to the equation come about when $x \equiv \pm 1 \pmod{p}$. □

Theorem 2.5. *Wilson's Theorem. If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. We know that $\{1, 2, \ldots, p\}$ is a reduced residue system modulo p, since $\phi(p) = p - 1$. Since we know that $a \equiv a^{-1} \pmod{p}$, which implies $aa^{-1} \equiv 1 \pmod{p}$ unless $a \equiv \pm 1 \pmod{p}$. This means that we can pair up elements in the system with their inverses and obtain:

$$(a_1 a_1^{-1})(a_2 a_2^{-1}) \ldots (a_k a_k^{-1}) \equiv (-1)(1) \equiv -1 \pmod{p} \tag{2.6}$$

This follows because the only factors of $(p-1)!$ which cannot be grouped into pairs equivalent to $1 \pmod{p}$ are 1 and -1. The theorem follows. □

Theorem 2.7. *The congruence $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof. The theorem follows trivially in the case when $p = 2$. Now, we will assume that $x^2 \equiv -1 \pmod{p}$. Assume by contradiction that there is a solution if $p \equiv 3 \pmod{4}$. We know that $p - 1 \equiv 2 \pmod{4}$. This implies that $p - 1 = 4k + 2$ for some $k \in \mathrm{N}$. Thus, we find that $x^{p-1} = x^{2(2k+1)} = (x^2)^{2k+1}$. Since we know that $x^2 \equiv -1 \pmod{p}$, we see that $x^{p-1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$ because $2k+1$ is odd. However, we see that $x^{p-1} \equiv 1 \pmod{p}$ by Fermat, which is a contradiction.

Now we shall assume that $p \equiv 1 \pmod{4}$. Then we know that $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. Now we can write this as:

$$(p-1)! \quad = \quad \left(1\ddot{2}\ddot{3}\ldots\frac{p-1}{2}\right)\left(\frac{p+1}{2}\cdot\frac{p+3}{2}\ldots(p-1)\right) \equiv -1 \pmod{p} \tag{2.8}$$

Let $x = 1\ddot{2}\ddot{3}\ldots\frac{p-1}{2}$, and so we need to show that $x \equiv \frac{p+1}{2} \cdot \frac{p+3}{2} \ldots (p-1) \pmod{p}$. Yet we know that $p - 1 \equiv (-1)(1) \pmod{p}$, $p - 2 \equiv (-1)(2) \pmod{p}$, $\ldots$, $\frac{p+1}{2} \equiv (-1)(\frac{p-1}{2}) \pmod{p}$. This shows that $\frac{p+1}{2} \cdot \frac{p+3}{2} \ldots (p-1) \pmod{p} \equiv (-1)^(p-1)(1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2}) \equiv x \pmod{p}$. This completes the theorem. □

Theorem 2.9. *Chinese Remainder Theorem: Given a system of congruences $x \equiv a_i \pmod{m_i}$ for $i \in \{1, \ldots, n\}$ such that all m_i are coprime in pairs, there exists a unique solution modulo $m_1 m_2 \ldots m_n$.*

Proof. First, we will show existence by constructing a number a which satisfies all of the congruences. Let $N_i = m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_n$. We know that $gcd(N_i, m_i) = 1$ because of the pairwise coprimeness. We can choose H_i such that $H_i N_i \equiv 1 \pmod{p}$. Now, we can set $a = H_1 N_1 a_1 + H_2 N_2 a_2 + \dots H_n N_n a_n$. It is obvious that $H_i N_i \equiv 0 \pmod{m_j}$ for all $j \neq i$, but we know that $H_i N_i \equiv 1 \pmod{m_i}$. This means that $a \equiv a_i \pmod{m_i}$ for all i. This completes the construction.

Second, we will show uniqueness. Suppose there are two solutions x and y such that $x \equiv a_i \pmod{m_i}$ and $y \equiv a \pmod{m_i}$. This shows that $x \equiv y \pmod{m_i}$, which shows that $x - y \equiv 0 \pmod{m_i}$. This implies that $m_i | x - y$ for all $i \in \{1, 2, \dots, n\}$. However, we know that $gcd(m_i, m_j) = 1$ for all $i \neq j$. This shows that $m_1 m_2 \dots m_n | x - y$. This means that $x \equiv y \pmod{m_1 m_2 \dots m_n}$. This shows uniqueness. □

Lemma 2.10. *For a polynomial $f(x) \in \mathrm{Z}[x]$, we must have $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$ for a prime p.*

Proof. We can take the taylor expansion of $f(a + tp^j)$, and we obtain:

$$f(a + tp^j) = f(a) + tp^j f'(a) + \frac{(tp^j)^2 f''(a)}{2!} + \dots \tag{2.11}$$

We know that $p^{j+1} | p^{kj}$ as long as $k \geq 2$. Moreover, we see that $f^{(k)}(a)/k!$ is an integer. This is because for any monomial we have $f^{(k)}(a) = (n)(n-1)\dots(n-k)a^{n-k}$. This means that $f^{(k)}(a)/k! = \binom{n}{k} a^{n-k}$, which is obviously an integer. □

Theorem 2.12. *Hansel's Lemma: Suppose that we have a solution $x = a$ of the polynomial $f(x) \equiv 0 \pmod{p^j}$. Suppose that $f(x) \in \mathrm{Z}[x]$, $f(a) \equiv 0 \pmod{p^j}$, and $f'(a) \not\equiv 0 \pmod{p}$. Then there exists a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

Proof. Using the lemma, we know that $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$. We want to set $f(a) + tp^j f'(a) \equiv 0 \pmod{p^{j+1}}$. This is equivalent to $tf'(a) + \frac{f(a)}{p^j} \equiv 0 \pmod{p}$. This means we can find a unique $t \equiv -\left(\frac{f(a)}{p^j}\right) \frac{1}{f'(a)} \pmod{p}$. This completes the proof. □

3. Primitive Roots

Lemma 3.1. *Let p be a prime. Suppose that $q^e || p - 1$ for some prime q. Then there exists an element modulo p of order q^e.*

Proof. Consider the solutions of $x^{q^e} \equiv 1 \pmod{p}$. We know that $q^e | p - 1$. We know that $x^{q^e} - 1$ has exactly q^e roots modulo p. If α is any such root, then $ord_p(a) | q^e$. Thus, if $ord_p(a) \neq q^e$, then we know that $ord_p(a) | q^e - 1$. Then we must have α be a root of $x^{q^{e-1}} \equiv 1 \pmod{p}$, which has exactly q^{e-1} solutions. Since $q^e - q^{e-1} > 0$, we know there exists α such that $ord_p(\alpha) = q^e$. □

Theorem 3.2. *There exist primitive roots modulo p where p is a prime.*

Proof. Write $p - 1 = q_1^{e_1} \dots q_r^{e_r}$. The lemma says that exists g_i such that $ord_p(g_i) = g_i^{e_i}$. Now let $g = g_1 g_2 \dots g_r$. By the lemma above, g has order $q_1^{e_1} \dots q_r^{e_r} = p - 1$, because $q_1^{e_1} \dots q_r^{e_r}$ are all coprime. Since $\phi(p) = p - 1$, we see that g is a primitive root modulo p. □

Theorem 3.3. *There's a primitive root modulo m if and only if $m = 1, 2, 4, p^e, 2p^e$ where p is an odd prime.*

4. Quadratic Reciprocity

Theorem 4.1. $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$ *if $p \nmid a$ and p is odd.*

Proof. We know that $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Since $p - 1$ is even, we must have $a^{((p-1)/2)^2} \equiv 1 \pmod{p}$. This implies that $a \equiv \pm 1 \pmod{p}$. Now let g be a primitive root modulo p. We know that $\{1, g, g^2, \dots, g^{p-1}\}$ runs through the entire residue system. This means that $a \equiv g^k \pmod{p}$ for some k. We also know that $a \equiv g^{k + m(p-1)} \pmod{p}$ so that k is only defined modulo $p - 1$.

Now we know that a is a quadratic residue modulo p if and only if k is even so that $g^k \equiv (g^{k/2})^2 \pmod{p}$. Now look at $a^{(p-1)/2} \equiv g^{k(p-1)/2} \pmod{p}$. We know that $g^{k(p-1)/2} \equiv 1 \pmod{p}$ if and only if $p - 1 | k(p-1)/2$. This occurs if and only if $p - 1 | k$, which occurs when $2 | k$. Thus, we see that $a^{(p-1)/2} \equiv 1 \pmod{p}$ exactly when a is a quadratic residue modulo p. □