

Math 115 - Midterm 1+2 Theorems

1. **Corollary.** Let $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$.
 - (a) $ab = c \iff \alpha(p) + \beta(p) = \gamma(p) \quad \forall p$.
 - (b) $a \mid c \iff \alpha(p) \leq \gamma(p) \quad \forall p$.
 - (c) c is a common divisor of a and b iff $\gamma(p) \leq \min(\alpha(p), \beta(p)) \quad \forall p$.
 - (d) $\gcd(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}$.
 - (e) $\text{lcm}(a, b) = \prod_p p^{\max(\alpha(p), \beta(p))}$.
 - (f) c is the square of an integer iff $\gamma(p)$ is even for all p .
2. **Pascal's Identity.** $\binom{\alpha+1}{k+1} = \binom{\alpha}{k+1} + \binom{\alpha}{k}$.
3. **Binomial Theorem.** $(x + y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i$.
4. **Theorem.** If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.
5. **Euler's Theorem.** If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.
6. **Fermat's Little Theorem.** Let p be a prime. Then:
 - (a) $\forall a \in \mathbb{Z}$ and a not a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.
 - (b) $\forall a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.
7. **Wilson's Theorem.** If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
8. **Solvability of $x^2 \equiv -1 \pmod{p}$.** Let p be a prime. Then, $x^2 \equiv -1 \pmod{p}$ has a solution $x \in \mathbb{Z}$ iff $p = 2$ or $p \equiv 1 \pmod{4}$.
9. **Fermat's Theorem on Sum of Squares.** Let p be a prime such that $p \equiv 1 \pmod{4}$. Then p can be written as $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$.
10. **Solving Degree 1 Congruences.** Let $a, b \in \mathbb{Z}$ and let $g = \gcd(a, m)$. Then:
 - (a) The congruence $ax \equiv b \pmod{m}$ has a solution iff $g \mid b$.
 - (b) If (a) is true, then $\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$ has a solution modulo $\frac{m}{g}$.
11. **Chinese Remainder Theorem.** If $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$ (where the m_i 's are pairwise relatively prime), then let $M = m_1 m_2 \cdots m_k$ and $y_i = \text{inverse} \left(\frac{M}{m_i} \pmod{m_i} \right)$. Then, a solution to the simultaneous congruence is given by $x \equiv a_1 \frac{M}{m_1} y_1 + \cdots + a_k \frac{M}{m_k} y_k \pmod{M}$.
12. **Theorem.** If $m \in \mathbb{Z}_{>0}$, then $\phi(m) = \left(\prod_{p \text{ prime}, p \mid m} \left(1 - \frac{1}{p}\right) \right) \cdot m$.
13. **RSA Cryptography Lemma.** Suppose $m \in \mathbb{Z}_{>0}$ and $\gcd(a, m) = 1$. Let $h, h' \in \mathbb{Z}_{>0}$ such that $hh' \equiv 1 \pmod{\phi(m)}$. Then $a^{kh'} \equiv a \pmod{m}$.
14. **Primality Testing.** If there is an integer a such that $0 < a < m$ and $a^{m-1} \not\equiv 1 \pmod{m}$, then m is not prime.

15. **Hensel's Lemma.** To solve the congruence $f(x) \equiv 0 \pmod{p^k}$, first find the solutions to $f(x) \equiv 0 \pmod{p}$. Then, for each solution a_1 to $f(x) \equiv 0 \pmod{p}$, "lift" its solution by the recurrence relation $a_2 = a_1 - f(a_1)\overline{f'(a_1)}$, where $\overline{f'(a_1)}$ is found by solving $f'(a_1)\overline{f'(a_1)} \equiv 1 \pmod{p}$ for $\overline{f'(a_1)}$. To higher powers, we generalize this recurrence relation to $a_{j+1} = a_j - f(a_j)\overline{f'(a_j)}$.
16. **Hensel's Lemma (General Case).** Let $f \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$, $j \in \mathbb{Z}_{>0}$, and $\tau \in \mathbb{N}$. Assume that $f(a) \equiv 0 \pmod{p^j}$, $p^\tau \parallel f'(a)$ and $j \geq 2\tau + 1$. Then:
 - (a) There is a $\tau \in \mathbb{Z}$, unique modulo p , such that $f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}}$.
 - (b) If $b \equiv a \pmod{p^{j-\tau}}$, then $f(b) \equiv f(a) \pmod{p^j}$ and $p^j \parallel f'(b)$.
17. **Corollary to Hensel's Lemma.** Let $f \in \mathbb{Z}[x]$, p be prime, $a \in \mathbb{Z}$, $\tau \in \mathbb{N}$, and let $l \in \mathbb{Z}$. Assume that $p^\tau \parallel f'(a)$, $f(a) \equiv 0 \pmod{p^l}$, and $l \geq 2\tau + 1$. Then, for any $\alpha \geq l$, there exists a $b \in \mathbb{Z}$, unique modulo $p^{\alpha-\tau}$, such that $b \equiv a \pmod{p^{l-\tau}}$ and $f(b) \equiv 0 \pmod{p^\alpha}$.
18. **Lemma.** Let $f \in \mathbb{Z}[x]$ and p prime. Assume that a_1, \dots, a_r are roots of $f \pmod{p}$, with $r > 0$ and $a_i \equiv a_j \pmod{p}$ for all $i \neq j$. Then there is a polynomial $g \in \mathbb{Z}[x]$ such that $f(x) \equiv (x - a_1)g(x) \pmod{p}$. Also, for any such g , a_1, \dots, a_r are roots of g modulo p .
19. **Theorem.** If $f(x) \equiv 0 \pmod{p}$ has (at least) r solutions $x \equiv a_1, \dots, a_r \pmod{p}$, with $a_i \not\equiv a_j \pmod{p}$ (for all $i \neq j$), then there is a polynomial $q \in \mathbb{Z}[x]$ such that $f(x) \equiv (x - a_1) \cdots (x - a_r)q(x) \pmod{p}$.
20. **Theorem 2.26.** The congruence $f(x) \equiv 0 \pmod{p}$ of degree $n \geq 0$ has at most n solutions.
21. **Corollary 2.27.** If $f \in \mathbb{Z}[x]$ has degree $n \geq 0$ (thus, $f \neq 0$), and the congruence $f(x) \equiv 0 \pmod{p}$ has more than n distinct solutions, then $f \equiv 0 \pmod{p}$ (as polynomials).
22. **Lemma.** Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n . If the congruence $f(x) \equiv 0 \pmod{p}$ has n solutions, $x \equiv a_1, \dots, a_n \pmod{p}$, distinct modulo p , then $f(x) \equiv (x - a_1) \cdots (x - a_n) \pmod{p}$.
23. **Proposition.** Let $f \in \mathbb{Z}[x]$. Then there is a well-defined function \tilde{f} with $\tilde{f} : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ given by $\tilde{f}(\tilde{a}) = \tilde{f(a)}$ for all $\tilde{a} \in \mathbb{Z}/m\mathbb{Z}$.
24. **Proposition.** Let $f, g \in \mathbb{Z}[x]$. If $f \equiv g \pmod{m}$ (as polynomials), then $\tilde{f} = \tilde{g}$ (as functions $\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$).
25. **Corollary.** Let $\psi : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ be any function. If ψ can be given by a polynomial (i.e. $\psi = \tilde{f}$ for some $f \in \mathbb{Z}[x]$), then it can be given by a polynomial of degree less than p .
26. **Theorem 2.28.** If $F : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, then there is a polynomial $f \in \mathbb{Z}[x]$ with degree at most $p - 1$ such that $F(x) \equiv f(x) \pmod{p}$ for all residue classes x modulo p .
27. **Theorem.** The polynomials in Theorem 2.28 are unique modulo p .
28. **Corollary 2.30.** Suppose $d > 0$ and $d \mid (p - 1)$, then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
29. **Proposition.** Let a have order h modulo m , and let $n \in \mathbb{N}$. Then, $a^n \equiv 1 \pmod{m}$ iff n is a multiple of h .
30. **Corollary.** If a has order h (modulo m), then $h \mid \phi(m)$.
31. **Corollary.** Let $m, m' \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. Assume that a has orders h and h' modulo m and m' , respectively (i.e. $\gcd(a, m) = \gcd(a, m') = 1$). Then, if $m \mid m'$, then $h \mid h'$.
32. **Proposition.** Suppose g is a primitive root modulo m . Then:
 - (a) $1, g, \dots, g^{\phi(m)-1}$ are distinct modulo m .

- (b) The above numbers are a reduced residue system modulo m .
- (c) Let $a \in \mathbb{Z}$, with $\gcd(a, m) = 1$. Then there exists an $i \in \mathbb{Z}$ such that for all $j \in \mathbb{N}$, $g^j \equiv a \pmod{m}$ iff $j \equiv i \pmod{\phi(m)}$.
33. If there exists a primitive root g modulo m , then you have a theory of discrete logarithms modulo m .
34. **Generalization of Corollary 2.30.** Assume that there is a primitive root modulo m and let d be a positive divisor of $\phi(m)$. Then, the congruence $x^d \equiv 1 \pmod{m}$ has exactly d solutions.
35. **Generalization of Theorem 2.37.** Assume that there is a primitive root modulo m and let $n \in \mathbb{Z}_{>0}$, and let $a \in \mathbb{Z}$ coprime to m . Then the congruence $x^n \equiv a \pmod{m}$ has $\gcd(n, \phi(m))$ solutions if $a^{\phi(m)/\gcd(n, \phi(m))} \equiv 1 \pmod{m}$ or has no solutions otherwise.
36. **Euler's Criterion.** Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Assume that there is a primitive root modulo p . Then, $x^2 \equiv a \pmod{p}$ has two solutions if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or has no solutions otherwise.
37. **Lemma.** Suppose $a \in \mathbb{Z}$ has order h modulo m . Then:
- (a) If $d > 0$, and $d \mid h$, then a^d has order $\frac{h}{d}$ modulo m .
- (b) For all $k \in \mathbb{N}$, a^k has order $\frac{h}{\gcd(h, k)} \pmod{m}$.
38. **Corollary.** If there is a primitive root modulo m , then there are $\phi(\phi(m))$ of them (as residue classes modulo m).
39. **Lemma.** Suppose that $a, b \in \mathbb{Z}$ have order h and k , respectively modulo m , and that h and k are coprime. Then, ab has order hk modulo m .
40. If p is prime, then there exists a primitive root modulo p .
41. **Lemma.** Let $m, m' \in \mathbb{Z}_{>0}$ with $m \mid m'$. Let $a \in \mathbb{Z}$, with $\gcd(a, m') = 1$. Then:
- (a) $\gcd(a, m) = 1$.
- (b) If h, h' are the orders of a and m' modulo m , respectively, then $h \mid h'$.
42. **Theorem.** Let p be an odd prime and let $\alpha \in \mathbb{Z}_{>0}$. Then there exists a primitive root modulo p^α .
43. **Diffie-Hellman Key Exchange.** This is a process used in order to initialize the secure line before message transfers occur. Suppose Alice and Bob are the participants. Then:
- (a) They (publicly) agree on a large prime p (600 digits...) and a primitive root g modulo p .
- (b) Alice thinks up a number a , $1 < a < p - 1$, and sends $g^a \pmod{p}$ to Bob.
- (c) Bob thinks up a number b , $1 < b < p - 1$, and sends $g^b \pmod{p}$ to Alice.
- (d) Alice computes $(g^b)^a \pmod{p}$ and Bob computes $(g^a)^b \pmod{p}$, which becomes their shared key.
44. **Solving Quadratic Congruences Modulo $p \neq 2$.** Let $ax^2 + bx + c \equiv 0 \pmod{p}$ be a quadratic congruence with $a \not\equiv 0 \pmod{p}$. First, multiply it by $\bar{a} \pmod{p}$ to get $x^2 + \bar{a}bx + \bar{a}c \equiv 0 \pmod{p}$. Then, complete the square to get $(x + \bar{2}ab)^2 + \bar{a}c - (\bar{2}ab)^2$. Then, solve the resulting congruence.
45. **Theorem 3.1.** Let $a, b \in \mathbb{Z}$. Then:
- (a) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
- (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

(c) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(d) If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = 1$ and $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

(e) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

46. **Theorem 3.2 (Lemma of Gauss).** Let $a \in \mathbb{Z}$ be relatively prime to p and let n be the number of elements of the set $\{j \in \{1, 2, \dots, p-1\} \mid ja \pmod{p} > \frac{p}{2}\}$. Then, $\left(\frac{a}{p}\right) = (-1)^n$.

47. **Part of Theorem 3.3.** Let $a \in \mathbb{Z}$ be relatively prime to p . Assume also that a is odd. Let $t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$. Then, $\left(\frac{a}{p}\right) = (-1)^t$.

48. **Quadratic Reciprocity.** We have:

(a) $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod{4}$ and -1 if $p \equiv -1 \pmod{4}$.

(b) $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod{8}$ and -1 if $p \equiv \pm 3 \pmod{8}$.

(c) For all odd primes p, q with $p \neq q$, we have that $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

49. START WITH 10/29/24 NOTES