

FINAL REVIEW
Math 104 - Dr. Evans
UCSD Winter 2004

In this handout, the basic definitions and theorems from Dr. Evans's class are stated in chronological order. Some sample problems are included at the end. These problems may or may not represent the problems on the final exam. The sample problems are not to be turned in.

1 Definitions

Congruence $a \equiv b \pmod{n}$ if $n|(a-b)$, or equivalently, if $a = b + kn$ for some integer k . See the original handout for the important properties of congruences.

Greatest Common Divisor d is a *greatest common divisor of a and b* if $d|a$, $d|b$, and for any other common divisor e of a and b , $e|d$. We say $d = \gcd(a, b)$ or sometimes just $d = (a, b)$.

Relatively Prime a and b are *relatively prime* if $\gcd(a, b) = 1$.

Quadratic Residues Suppose $a \not\equiv 0 \pmod{p}$ for an odd prime p . Then a is a *quadratic residue modulo p* if $a \equiv x^2 \pmod{p}$ has a solution. Quadratic residues are also called *squares modulo p* . For a given p , the quadratic residues are

$$\left\{1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2\right\}.$$

Legendre Symbol Let p be an odd prime and a be any integer not divisible by p . The *Legendre symbol* $\left(\frac{a}{p}\right)$ is 1 if a is a square modulo p and -1 if a is not a square modulo p . The Legendre Symbol has the following properties:

- If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- For any a, b not divisible by p , $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Jacobi Symbol The Jacobi symbol is the same as the Legendre symbol, except the number on the bottom does not need to be a prime, just odd. If n is a positive odd integer, let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Then for any a relatively prime to n , the *Jacobi symbol* is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_r}\right)^{e_r}$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol. The Jacobi symbol has the same properties as the Legendre symbol, plus one more:

- For any odd integers m and n , and a relatively prime to mn , $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Note that the Jacobi symbol $\left(\frac{a}{n}\right) = 1$ does *not* mean that a is a square modulo n . For example, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, but 2 is not a square modulo 15. However, in conjunction with

quadratic reciprocity, it can be used to prove other statements without knowing the factorization of the bottom number. For example,

$$\left(\frac{15}{17}\right) = \left(\frac{17}{15}\right) = \left(\frac{2}{15}\right) = 1$$

since $15 \equiv -1 \pmod{8}$. Hence, we can say 15 is a square modulo 17 without needing to know how 15 factors.

Algebraic Integers An *algebraic integer* in $\mathbb{Q}(\sqrt{m})$ is either $a + b\sqrt{m}$ where a and b are integers, or if $m \equiv 1 \pmod{4}$, then in addition $\frac{a+b\sqrt{m}}{2}$ where a and b are odd integers. For example, $\frac{3+\sqrt{5}}{2}$ and $\frac{1-5\sqrt{-3}}{2}$ are algebraic integers, but $\frac{1+\sqrt{3}}{2}$ and $\frac{2+\sqrt{5}}{2}$ are not algebraic integers.

More generally, any algebraic integer satisfies some monic polynomial, meaning that all the coefficients of a polynomial are integers and the coefficient of the highest power is 1. For example, $\sqrt{3} + \sqrt{5}$ is an algebraic integer since it satisfies the polynomial $x^4 - 16x^2 + 4 = 0$.

Norm The *norm* of $\alpha = a + b\sqrt{m}$ is $N(\alpha) = \alpha\alpha' = a^2 - mb^2$, where $\alpha' = a - b\sqrt{m}$ is called the *conjugate* of α .

Order The *order* of $\alpha = a + b\sqrt{m}$ modulo p for an integer prime p is the smallest positive integer e such that $\alpha^e \equiv 1 \pmod{p}$ (as long as $N(\alpha)$ is relatively prime to p).

Euler ϕ Function For any positive integer n , define $\phi(n)$ to be the number of integers between 1 and n which are relatively prime to n . $\phi(n)$ is the number of elements in $U(n) = \{1 \leq a \leq n \mid \gcd(a, n) = 1\}$.

2 Theorems

Unique Factorization of Integers Every positive integer n has a unique factorization into prime numbers. If $n = p_1^{e_1} \cdots p_r^{e_r}$ and $n = q_1^{f_1} \cdots q_s^{f_s}$ are two prime factorizations of n , then $r = s$ and for all i , $p_i = q_j$ and $e_i = f_j$ for some j (i.e., the prime factors and exponents are unique up to reordering).

Euclidean Algorithm For any positive integers a and b , there exists a unique q and r such that $a = bq + r$ and $0 \leq r < b$.

Facts about $\gcd(a, b)$ Suppose a and b are positive integers.

- $\gcd(a, b) = \min\{ax + by > 0 \mid x, y \in \mathbb{Z}\}$.
- $\gcd(a, b)$ can be written as a linear combination of a and b .
- a and b are relatively prime if and only if there exist integers m and n such that $am + bn = 1$.
- a has an inverse modulo b if and only if a and b are relatively prime.

Fermat's Little Theorem For any prime p and any integer a not divisible by p , $a^{p-1} \equiv 1 \pmod{p}$. Alternatively, $a^p \equiv a \pmod{p}$ for all a .

Wilson's Theorem For any prime p , $(p-1)! \equiv -1 \pmod{p}$.

Euler's Criterion For any odd prime p and any integer a not divisible by p , then a is a square modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. More specifically,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{if } a \text{ is a square modulo } p \\ -1 \pmod{p} & \text{if } a \text{ is not a square modulo } p \end{cases}$$

Using the definition of the Legendre symbol, Euler's Criterion may be stated as

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

Products of Squares and Nonsquares

- If a and b are squares modulo p , then ab is a square modulo p .
- If a is a square and b is not a square modulo p , then ab is not a square modulo p .
- If a and b are both not squares modulo p , then ab is a square modulo p .

Quadratic Reciprocity Let p and q be distinct odd primes.

Main Case

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \end{cases}$$

Special Case 1

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

Special Case 2

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Chinese Remainder Theorem Let m and n be relatively prime positive integers. Given the congruence equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

there exists a unique $0 \leq c \leq mn - 1$ such that

$$x \equiv c \pmod{mn}$$

The solution is given by $x = an(n^{-1} \pmod{m}) + bm(m^{-1} \pmod{n})$.

Let p , q , and r be pairwise relatively prime positive integers. Given the congruence equations

$$\begin{aligned}x &\equiv a \pmod{p} \\x &\equiv b \pmod{q} \\x &\equiv c \pmod{r}\end{aligned}$$

then a solution modulo pqr is given by

$$x = aqr((qr)^{-1} \pmod{p}) + bpr((pr)^{-1} \pmod{q}) + cpq((pq)^{-1} \pmod{r})$$

Legendre's Theorem Given squarefree positive integers a , b , and c which are pairwise relatively prime, then $ax^2 + by^2 = cz^2$ has a solution in the integers if and only if bc is a square modulo a , ac is a square modulo b , and $-ab$ is a square modulo c .

Fermat's Little Theorem for $a + b\sqrt{m}$ Let $\alpha = a + b\sqrt{m}$ be an algebraic integer, $\alpha' = a - b\sqrt{m}$ is its conjugate. Then for any prime p which is relatively prime to m ,

$$\alpha^p \equiv \begin{cases} \alpha \pmod{p} & \text{if } \left(\frac{m}{p}\right) = 1 \\ \alpha' \pmod{p} & \text{if } \left(\frac{m}{p}\right) = -1 \end{cases}$$

Lucas-Lehmer Test Let p be an odd prime, and let $q = 2^p - 1$. Define the sequence S_n by setting $S_1 = 4$ and $S_n = (S_{n-1})^2 - 2$ for all $n \geq 2$. Then q is a prime if and only if $S_{p-1} \equiv 0 \pmod{q}$.

Facts about Euler ϕ Function

- For any prime p , $\phi(p) = p - 1$.
- For any prime p and positive integer k , $\phi(p^k) = p^k - p^{k-1}$.
- If m and n are positive relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.
- For any integer $n > 1$ and integer a relatively prime to n , $a^{\phi(n)} \equiv 1 \pmod{n}$. Hence, the order of a modulo n divides $\phi(n)$.

3 Sample Problems

1. Show that $\mathbb{Z}[\sqrt{-26}]$ does not have unique factorization by factoring 27 in two different ways. Make sure you prove your factors are "prime."
2. Let n be a positive integer greater than 1, and let a be an integer relatively prime to n . Show that $\{ka \mid 1 \leq k \leq n - 1, \gcd(k, n) = 1\}$ are all distinct modulo n .
3. Suppose p is an odd prime and a , b , and n are positive integers with $n > 1$ squarefree. Show that if $p = a^2 + nb^2$, then a and b are unique. Show that a and b are *not* unique for $4p = a^2 + 3b^2$. (Hint: Try $p = 7$.)
4. Compute the order of $\phi = \frac{1+\sqrt{5}}{2}$ modulo 7 and modulo 11. (Hint: Use Fermat's Little Theorem and $\phi' = -\frac{1}{\phi}$.)
5. Use the Lucas-Lehmer test to show that $2^{11} - 1$ is not prime and $2^{13} - 1$ is a prime. (It's okay to use a calculator on this one.)