WON Series in Discrete Mathematics and Modern Algebra Volume 2

NUMBER THEORY

Amin Witno

These notes have been prepared for students of Math 313 at Philadelphia University, Jordan.[1] Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

1 Divisibility

Definition. Let $d, m \in \mathbb{Z}$. If $m/d \in \mathbb{Z}$, then we say that d *divides* m, and that m is *divisible by* d. We write $d \mid m$ when d divides m, or $d \nmid m$ otherwise.

Example. We have $3 \mid 15$ and $10 \mid 20$. Also $3 \nmid 22$ and $5 \nmid 21$.

Theorem 1.1. The following are some properties of divisibility.

1. We have $1 \mid m$ for all $m \in \mathbb{Z}$.
2. If $d \neq 0$, then $d \mid d$ and $d \mid 0$.
3. If $d \mid m$ and $m \mid n$, then $d \mid n$.
4. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$ for all $a, b \in \mathbb{Z}$.

Proof. In class. ▽

Definition. For all $x \in \mathbb{R}$, the *floor* of x is defined to be the greatest integer $n \leq x$.

Example. We have $\lfloor 3.14 \rfloor = 3$ and $\lfloor 20/3 \rfloor = 6$. Also $\lfloor 2 \rfloor = 2$ and $\lfloor -3.14 \rfloor = -4$.

Problem 1. Evaluate the floor function.
(a) $\lfloor 3.999 \rfloor$ (b) $\lfloor \sqrt{450} \rfloor$ (c) $\lfloor 234/9 \rfloor$ (d) $\lfloor -99/7 \rfloor$

Definition. With $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we define m *mod* n as

$$m \,\%\, n = m - \left\lfloor \frac{m}{n} \right\rfloor \times n$$

Note that $m \,\%\, n$ is just the remainder upon dividing m by n using the long division algorithm taught in grade school.

Last Revision: 02–01–2019
awitno@gmail.com

Example. We have $20 \,\%\, 3 = 2$ and $100 \,\%\, 13 = 9$. Also $7 \,\%\, 11 = 7$ and $24 \,\%\, 8 = 0$.

Problem 2. Evaluate the mod operation.
(a) $123456789 \,\%\, 10$ (b) $100 \,\%\, 7$ (c) $-111 \,\%\, 22$ (d) $12345 \,\%\, 15$

Theorem 1.2. The following are some properties of the mod operator.

1. We have $0 \leq m \,\%\, n \leq n - 1$.
2. If $0 \leq m < n$, then $m \,\%\, n = m$.
3. We have $m \,\%\, n = 0$ if and only if $n \mid m$.
4. If $m = qn + r$ with $0 \leq r \leq n - 1$, then $r = m \,\%\, n$ and $q = \lfloor m/n \rfloor$.

Proof. In class. ▽

Definition. According to Theorem 1.2, for all $n \in \mathbb{Z}$ either $n \,\%\, 2 = 0$ or $n \,\%\, 2 = 1$. We call such numbers *even* or *odd,* respectively. Thus n is even if $n = 2k$, and odd if $n = 2k + 1$, for some $k \in \mathbb{Z}$.

Problem 3. Prove that (a) $8 \mid n^2 - 1$ if n is odd (b) $4 \nmid n^2 + 2$ for all n even or odd.

Theorem 1.3. One in every k consecutive integers is divisible by k.

Proof. Consider the consecutive integers $n, n + 1, \ldots, n + k - 1$, and let $n \,\%\, k = d$. If $d = 0$, we are done; otherwise $1 \leq d \leq k - 1$. Since $n - d = \lfloor n/k \rfloor k$, we have $k \mid n - d$ and also, by Theorem 1.1, $k \mid n + k - d$. And since $1 \leq k - d \leq k - 1$, then $n + k - d$ is one of the consecutive integers. ▽

Example. Prove that $2 \mid n^2 - n$ and $3 \mid n^3 - n$ for all $n \in \mathbb{Z}$.
Solution. We have $n^2 - n = (n-1)n$, of two consecutive integers, hence divisible by 2. Similarly, $n^3 - n = (n-1)n(n+1)$ has three consecutive integers, hence divisible by 3.

Problem 4. Prove that (a) $4 \mid n^4 - n^2$ and (b) $5 \mid n^5 - n$ for all $n \in \mathbb{Z}$.

Definition. When $d \mid m$, we say that d is a *divisor* of m, and that m is a *multiple* of d. In a most usual context, the term divisor is understood positive divisor.

Example. The number 11 is a divisor of 77, and 45 is a multiple of 5 and of 9.

Definition. With $m, n \in \mathbb{Z}$, not both zeros, we define $\gcd(m, n)$ to be the greatest common divisor of m and n, i.e., the largest integer d such that $d \mid m$ and $d \mid n$.

Example. We have $\gcd(24, 56) = 8$ because $8 \mid 24$ and $8 \mid 56$, and because there is no other divisor of 24 and 56 that is larger than 8.

Theorem 1.4. If $n \in \mathbb{N}$, then $\gcd(m, n) = \gcd(n, m \,\%\, n)$.

Proof. Let $M = m \,\%\, n = m - \lfloor m/n \rfloor n$, and set

$$L = \{d \in \mathbb{Z} : d \mid m \text{ and } d \mid n\}$$
$$R = \{d \in \mathbb{Z} : d \mid n \text{ and } d \mid M\}$$

To prove the theorem, we will show that $L = R$. Suppose $d \in L$. Since $d \mid m$ and $d \mid n$, by Theorem 1.1 we have $d \mid am + bn = M$, where $a = 1$ and $b = -\lfloor m/n \rfloor$. Hence $d \in R$. Conversely, suppose $d \in R$. Since $d \mid n$ and $d \mid M$, then $d \mid an + bM = m$, where $a = \lfloor m/n \rfloor$ and $b = 1$. Hence $d \in L$, and the result follows. ▽

Example (The Euclidean Algorithm). Let $m = 201$ and $n = 72$. Repeated application of Theorem 1.4 generates the identities

$$\gcd(201, 72) = \gcd(72, 57) = \gcd(57, 15) = \gcd(15, 12) = \gcd(12, 3) = \gcd(3, 0) = 3$$

To shorten the writing, we record only the sequence of remainders:

$$201, 72, 57, 15, 12, 3, 0$$

noting that each term is obtained via the mod operation:

$$\begin{aligned} 201 - (2) \times 72 &= 57 \\ 72 - (1) \times 57 &= 15 \\ 57 - (3) \times 15 &= 12 \\ 15 - (1) \times 12 &= 3 \\ 12 - (4) \times 3 &= 0 \end{aligned}$$

According to Theorem 1.2, such a sequence is strictly decreasing hence must terminate with zero, which is necessarily preceded by $\gcd(m, n)$, as $\gcd(d, 0) = d$ for any $d \in \mathbb{N}$.

Problem 5. Evaluate $\gcd(m, n)$.
(a) $\gcd(549, 81)$ (b) $\gcd(1234, 5678)$ (c) $\gcd(234, 60970)$ (d) $\gcd(12345, 54321)$

Theorem 1.5. There exist $a, b \in \mathbb{Z}$ such that $\gcd(m, n) = am + bn$.

Proof. We observe that if $M = a_1 m + b_1 n$ and $N = a_2 m + b_2 n$, then

$$aM + bN = (aa_1 + ba_2)m + (ab_1 + bb_2)N$$

i.e., a linear combination of two linear combinations of m and n is again a linear combination of m and n. Now the resulting sequence $\{a_k \mid k \geq 0\}$ upon applying the euclidean algorithm obeys the recurrence $a_k = a_{k-2} \,\%\, a_{k-1}$ for all $k \geq 2$. This says that a_k is a linear combination of a_{k-2} and a_{k-1}. And since $a_0 = m = 1m + 0n$ and $a_1 = n = 0m + 1n$, we see that every term in $\{a_k\}$, and $\gcd(m, n)$ in particular, is a linear combination of m and n. ▽

Example (The Extended Euclidean Algorithm). We repeat the euclidean algorithm for computing $\gcd(201, 72)$, this time expressing each remainder as a linear combination of the form $d = (a)\,201 + (b)\,72$.

	d	a	b
	201	1	0
– (2)	72	0	1
– (1)	57	1	–2
– (3)	15	–1	3
– (1)	12	4	–11
– (4)	3	–5	14
	0		

The row above $d = 0$ easily checks that $\gcd(201, 72) = 3 = (-5)\,201 + (14)\,72$.

Problem 6. Find integers a and b such that $\gcd(m,n) = am + bn$.
(a) $\gcd(27, 25)$ (b) $\gcd(549, 81)$ (c) $\gcd(345, 215)$ (d) $\gcd(843, 2890)$

Problem 7. Prove that if $d \mid m$ and $d \mid n$, then $d \mid \gcd(m,n)$.

Theorem 1.6. Suppose that $\gcd(c,d) = 1$. If $c \mid m$ and $d \mid m$, then $cd \mid m$.

Proof. By Theorem 1.5, there are $a, b \in \mathbb{Z}$ such that $1 = ac+bd$. Multiply this equality by m/cd and we get $m/cd = a(m/d)+b(m/c)$, which is an integer if $m/c, m/d \in \mathbb{Z}$. $\bigtriangledown$

Example. Prove that $6 \mid n^3 - n$ for all $n \in \mathbb{Z}$.
Solution. We are not getting six consecutive out of $n^3 - n$. However, $6 = 2 \times 3$ with $\gcd(2,3) = 1$, so by the theorem it suffices to prove that $2 \mid n^3 - n$ and $3 \mid n^3 - n$. Both are a consequence of the fact that we have a product of three consecutive integers.

Problem 8. Prove that if n is odd, then $24 \mid n^3 - n$.

Problem 9. Prove that (a) $30 \mid n^5 - n$ and (b) $120 \mid (n^3 - n)(n^2 - 4)$ for all $n \in \mathbb{Z}$.

Theorem 1.7. There exist $a, b \in \mathbb{Z}$ with $am + bn = 1$ if and only if $\gcd(m,n) = 1$.

Proof. If $\gcd(m,n) = 1$, then $1 = am + bn$ for some $a, b \in \mathbb{Z}$ by Theorem 1.5. Conversely, let $a, b \in \mathbb{Z}$ such that $am + bn = 1$. If $d = \gcd(m,n)$, then by definition $d \mid m$ and $d \mid n$, hence $d \mid am + bn$ by Theorem 1.1. Thus $d \mid 1$, and so $d = 1$. $\bigtriangledown$

Problem 10. Prove the propositions:
(a) If $\gcd(m,n) = d$, then $\gcd(m/d, n/d) = 1$.
(b) If $\gcd(m,n) = am + bn$, then $\gcd(a,b) = 1$.
(c) If $\gcd(a,m) = 1$ and $\gcd(a,n) = 1$, then $\gcd(a,mn) = 1$.

Theorem 1.8 (Euclid's Lemma)**.** If $d \mid mn$ and $\gcd(d,m) = 1$, then $d \mid n$.

Proof. Let $d \mid mn$ and $\gcd(d,m) = 1$. By Theorem 1.5, $1 = ad+bm$ for some $a, b \in \mathbb{Z}$. It follows that $n/d = an + b(mn/d) \in \mathbb{Z}$ and $d \mid n$. $\bigtriangledown$

Theorem 1.9. Let $d = \gcd(m,n)$. Then the linear equation $mx + ny = c$ has a solution if and only if $d \mid c$, in which case all its solutions are given by $x = x_0 + kn/d$ and $y = y_0 - km/d$, for any particular solution (x_0, y_0) and for any $k \in \mathbb{Z}$.

Proof. From Calculus, the solutions of the linear equation form the straight line passing through (x_0, y_0) with a slope of $-m/n$. Every point on this line is given by $(x_0+t, y_0 - tm/n)$, with $t \in \mathbb{R}$. We have integer solution if and only if $t \in \mathbb{Z}$ and $n \mid tm$. Note first that if $d = 1$, then Euclid's lemma demands that $n \mid t$, i.e., $t = kn$ for any $k \in \mathbb{Z}$, giving the general solution $x = x_0 + kn$ and $y = y_0 - km$. For $d \geq 1$ in general, we replace our equation by $(m/d)x + (n/d)y = c/d$ without altering its solution set. But then $\gcd(m/d, n/d) = 1$ (Problem 10), and therefore the general solution is $x = x_0 + kn/d$ and $y = y_0 - km/d$. $\bigtriangledown$

Example. Find all solutions $x, y \in \mathbb{Z}$ such that $201x + 72y = 21$.
Solution. We return to the extended euclidean algorithm where we get $\gcd(201, 72) = 3 = (-5)\,201 + (14)\,72$. Since $3 \mid 21$, solution exists. In fact, multiplying this equation by 7 gives $21 = (-35)\,201 + (98)\,72$, i.e., $x_0 = -35$ and $y_0 = 98$. The general solution is therefore $x = -35 + 24k$ and $y = 98 - 67k$.

Problem 11. Solve the linear equation, if a solution exists.
(a) $34x + 55y = 1$ (b) $24x + 18y = 44$ (c) $25x + 85y = -35$ (d) $48x - 28y = 32$

2 Primes

Definition. To *factor* a number $n \in \mathbb{N}$ means to express n as the product of two or more smaller numbers, e.g., $n = a \times b$ with $1 < a, b < n$. Here we say that a and b are factors of n. Thus a factor of n means a divisor d in the range $2 \le d \le n/2$. The term *factorization* is also used to describe the act of factoring.

If $n \ge 2$, we call n a *prime* if n cannot be factored, and *composite* if it can.

Example. From 2 to 313, the primes are listed below and the composites are not.

2	3	5	7	11	13	17	19	23	29	31	37	41
43	47	53	59	61	67	71	73	79	83	89	97	101
103	107	109	113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199	211	223	227	229	233	239
241	251	257	263	269	271	277	281	283	293	307	311	313

Problem 12. Prove that every prime number is odd except 2.

Theorem 2.1. The following are some properties of factorization.

1. Every composite has a prime factor.
2. Every composite n has a prime factor $p \le \sqrt{n}$.
3. Every composite can be factored into a product of prime numbers.

Proof. In class. ▽

Example (Trial Division Algorithm). We illustrate how to determine primality for a small number, say $n = 317$. According to Theorem 2.1, if 317 is composite, then it has a prime factor $p \le \sqrt{3}17 \approx 17.80$, i.e., $p \in \{2, 3, 5, 7, 11, 13, 17\}$. We try all and find that $p \nmid 317$ in this range. Hence, we know that 317 is prime. Of course, if $p \mid n$ during the trial, then not only we know that n is composite but also have a factorization.

Problem 13. Determine prime or composite using trial division.
(a) 323 (b) 799 (c) 811 (d) 1333

Example (Fermat Factorization Algorithm). Sometimes a composite n may have no small factors, e.g., when its factors are in the proximity of $\sqrt{n}$. We illustrate how to factor $n = 4183$ by trying to find $x, y \in \mathbb{Z}$ such that $x^2 - n = y^2$, which will then give $n = (x+y)(x-y)$. Since $\sqrt{4183} \approx 64.67$, we start with $x = 65, 66, \ldots$ until y is found:

$$\begin{aligned} 65^2 - 4183 &= 42 \\ 66^2 - 4183 &= 173 \\ 67^2 - 4183 &= 306 \\ 68^2 - 4183 &= 441 = 21^2 \end{aligned}$$

We conclude with $4183 = 68^2 - 21^2 = (68 + 21)(68 - 21) = 89 \times 47$.

Problem 14. Factor n using Fermat factorization.
(a) 2117 (b) 16781 (c) 17933 (d) 70027

Theorem 2.2. For every $n \in \mathbb{Z}$, if p is a prime number, then

$$\gcd(p, n) = \begin{cases} p & \text{if } p \mid n \\ 1 & \text{if } p \nmid n \end{cases}$$

Proof. This is obvious since the only divisors of p are 1 and p. ▽

Theorem 2.3. Let p be a prime. If $p \mid mn$, then either $p \mid m$ or $p \mid n$.

Proof. If $p \nmid n$, then $\gcd(p, n) = 1$ and so if $p \mid mn$, then $p \mid m$ by Euclid's lemma. ▽

Problem 15. Prove that if a prime $p \mid n^2$, then $p^2 \mid n^2$.

Theorem 2.4 (The Fundamental Theorem of Arithmetic)**.** Every composite is the product of a unique collection of prime numbers, counting multiplicity.

Proof. By contradiction, suppose that a composite has factored into two distinct multisets of primes. After canceling common factors, we would have $\prod p_j = \prod q_k$ with primes p_j and q_k not having a common value. Theorem 2.3 implies that each p_j divides one q_k, and it is absurd to have a prime dividing another prime. ▽

Example. Let $n = 7920$. The prime factorization $n = 2^4 \times 3^2 \times 5 \times 11$ is unique. Moreover, if $d \mid n$, by the uniqueness of the prime factorization of d plus Theorem 2.3, we must have $d = 2^{e_2} \times 3^{e_3} \times 5^{e_5} \times 11^{e_{11}}$, where $e_2 \in \{0, 1, 2, 3, 4\}, e_3 \in \{0, 1, 2\}, e_5 \in \{0, 1\}, e_{11} \in \{0, 1\}$. There is a total of $5 \times 3 \times 2 \times 2 = 60$ divisors of n.

Problem 16. Determine the number of divisors of n.
(a) 720 (b) 1024 (c) 2310 (d) 19392

Example. Suppose that m and n have been factored into primes, e.g.,

$$\begin{aligned} m &= 2^7 \times 3^2 \times 7 \times 11^3 \\ n &= 2^3 \times 3^5 \times 5^4 \times 7^6 \end{aligned}$$

If $d \mid m$ and $d \mid n$, then d must factor into primes that are common to those of m and n, i.e., $d = 2^{e_2} \times 3^{e_3} \times 7^{e_7}$, where $e_2 \in \{0, 1, 2, 3\}, e_3 \in \{0, 1, 2\}, e_7 \in \{0, 1\}$. The largest such d is therefore $\gcd(m, n) = 2^3 \times 3^2 \times 7 = 504$.

Problem 17. Evaluate $\gcd(m, n)$ using prime factorization.
(a) $\gcd(40, 72)$ (b) $\gcd(1210, 1024)$ (c) $\gcd(19845000, 893025)$ (d) $\gcd(19392, 29391)$

Theorem 2.5. There are infinitely many prime numbers.

Proof. Given a set S of primes, let $n = 1 + \prod_{p \in S} p$. Since $n > p$ for all $p \in S$, either n is a new prime or else n has a prime factor $q \mid n$. If $q \in S$, then $q \mid \prod_{p \in S} p$ and then $q \mid n - \prod_{p \in S} p = 1$, which is impossible as q is prime. Hence $q \notin S$, and the claim holds since $|S|$ is arbitrary. ▽

Definition. For $x \in \mathbb{R}$, let $\pi(x)$ count the number of primes $p \leq x$.

Example. We have $\pi(11) = 5$ and $\pi(313) = 65$. Also $\pi(\pi) = 2$.

Theorem 2.6 (The Prime Number Theorem)**.** If $\log x$ denotes the natural logarithm function, then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

This means that if x is sufficiently large, then we may use $x/\log x$ to estimate the value of $\pi(x)$ with a small relative error.

Proof. Not here. ▽

Example. The number of primes below one million has been determined to be $\pi(10^6) = 78498$. For comparison, our scientific calculator reveals that $10^6/\log(10^6) \approx 72382.41$.

Problem 18. Estimate the number of primes that have exactly nine decimal digits.

Theorem 2.7 (Dirichlet's Theorem)**.** For a fixed $n \in \mathbb{N}$, there exist infinitely many primes p with remainder $p \,\%\, n = a$ if and only if $\gcd(a, n) = 1$.

Proof. Not here. ▽

Example. Prove that there are infinitely many primes p such that $p \,\%\, 4 = 3$.
Solution. Observe that a prime $p > 2$ must have the form $4n + 1$ or $4n + 3$. Moreover, the product of two numbers of the form $4n + 1$ is again of the same form, hence a number of the form $4n + 3$ must have a prime divisor of the form $4n + 3$. Now let S be a given set of primes of the form $4n + 3$. Set $N = 4\left(-1 + \prod_{p\in S} p\right) + 3$ with a prime factor q of the form $4n + 3$. Then $q \notin S$ or else $q \mid N - 4\prod_{p\in S} p = -1$, which is false. Hence such primes are infinite.

3 Congruences

Definition. We say that $a, b \in \mathbb{Z}$ are *congruent* to each other *modulo* n when $a \,\%\, n = b \,\%\, n$. We write $a \equiv b \pmod n$ if this is so, or $a \not\equiv b \pmod n$ otherwise.

Example. We have $27 \equiv 42 \pmod 5$ and $13 \not\equiv 8 \pmod 3$. Also, we have $a \equiv b \pmod 2$ if and only if both a and b are even or both odd.

Theorem 3.1. We have $a \equiv b \pmod n$ if and only if any one condition below holds.

1. $n \mid (a - b)$
2. $a - b \equiv 0 \pmod n$
3. $a = b + nk$ for some $k \in \mathbb{Z}$

Proof. In class. ▽

Problem 19. Prove that if a is odd, then $a^2 \equiv 1 \pmod 8$.

Problem 20. Prove that if $a \equiv b \pmod n$, then $\gcd(a, n) = \gcd(b, n)$.

Theorem 3.2. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$ and $ac \equiv bd \pmod n$, hence also $f(a) \equiv f(b) \pmod n$ for any polynomial $f(x)$ with integer coefficients.

Proof. In class. ▽

Problem 21. Prove that if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{mn}$, under the condition that $\gcd(m, n) = 1$.

Theorem 3.3. If $\gcd(m, n) = 1$ and $ma \equiv mb \pmod{n}$, then $a \equiv b \pmod{n}$.

Proof. Since $ma \equiv mb \pmod{n}$ means $n \mid ma - mb = m(a - b)$, then if $\gcd(m, n) = 1$, Euclid's lemma implies $n \mid (a - b)$, that is $a \equiv b \pmod{n}$. ▽

Definition. For each $m \in \{0, 1, \ldots, n-1\}$, define the *residue class* of m modulo n to be the set $[m]_n = \{x \in \mathbb{Z} \mid x \,\%\, n = m\}$. Thus $a, b \in \mathbb{Z}$ belong in the same class if and only if $a \equiv b \pmod{n}$, and therefore a residue class is also called *congruence class*. Furthermore, we may write

$$[m]_n = \{x \in \mathbb{Z} \mid x \equiv m \pmod{n}\} = \{m + nk \mid k \in \mathbb{Z}\}$$

Observe that the n classes $[0]_n, [1]_n, \ldots, [n-1]_n$ form a partition on $\mathbb{Z}$, so we hereby extend this definition for all $m \in \mathbb{Z}$ by letting $[m]_n = [m \,\%\, n]_n$.

Example. We have $[0]_2 = \{2k \mid k \in \mathbb{Z}\}$ and $[1]_2 = \{1 + 2k \mid k \in \mathbb{Z}\}$, which partition the integers into even and odd numbers. Also $[17]_3 = [2]_3 = \{\ldots, 2, 5, 8, 11, 14, 17, \ldots\}$.

Problem 22. Prove that if a prime $p \in [1]_3$, then $p \in [1]_6$.

Theorem 3.4. Let $d = \gcd(m, n)$. Then the linear congruence $mx \equiv c \pmod{n}$ has a solution if and only if $d \mid c$, in which case all its solutions are given by $x \in [x_0]_{n/d}$ for any particular solution $x_0 \in \mathbb{Z}$.

Proof. We have $mx_0 \equiv c \pmod{n}$ if and only if there exists $y_0 \in \mathbb{Z}$ such that $mx_0 + ny_0 = c$. Theorem 1.9 gives the general solution $x = x_0 + kn/d$, i.e., $x \in [x_0]_{n/d}$. ▽

Example. Find all $x \in \mathbb{Z}$ satisfying $24x \equiv 54 \pmod{126}$
Solution. We resort to the extended euclidean algorithm and arrive at $\gcd(24, 126) = 6 = 24\,(-5) + 42\,(1)$. Since $6 \mid 54$, we may multiply the linear combination by the integer 9 to get $54 = 24\,(-45) + 42\,(9)$. By Theorem 1.9, the general solution is $x = -45 + 21k$, which is equivalent to $x \in [18]_{21}$.

Problem 23. Solve the linear congruence, if a solution exists.
(a) $8x \equiv 5 \pmod{13}$ (b) $35x \equiv 7 \pmod{49}$ (c) $6x \equiv 9 \pmod{1023}$
(d) $19392x \equiv 6666 \pmod{29391}$

Definition. When $ab \equiv 1 \pmod{n}$, we call the numbers a and b *inverses* of each other modulo n. Observe that an inverse of a is also an inverse of every $x \in [a]_n$.

Example. The number 3 is an inverse of 5 modulo 7 because $3 \times 5 \equiv 1 \pmod{7}$. Also, 5 is its own inverse modulo 8.

Theorem 3.5. The number a has an inverse modulo n if and only if $\gcd(a, n) = 1$, in which case all its inverses belong to a unique residue class modulo n.

Proof. This follows from Theorem 3.4 by letting $m = a$ and $c = 1$. ▽

Definition. If $ab \equiv 1 \pmod{n}$, we denote the *inverse class* of a modulo n by $[a^{-1}]_n = [b]_n$ and the *inverse* of a *mod* n by $a^{-1} \,\%\, n = b \,\%\, n$. Sometimes we also write $a^{-1} \bmod n$ when refering to an element in this inverse class.

Example. Evaluate $13^{-1} \,\%\, 100$.
Solution. The problem is equivalent to solving the linear congruence $13x \equiv 1 \pmod{100}$ and the linear equation $13x + 100y = 1$. Our algorithm returns $1 = 13\,(-23) + 100\,(3)$, thus the inverse class $[-23]_{100}$. Hence, $13^{-1} \,\%\, 100 = -23 \,\%\, 100 = 77$.

Problem 24. Evaluate the inverse mod, if exists.
(a) $64^{-1} \,\%\, 81$ (b) $28^{-1} \,\%\, 89$ (c) $27^{-1} \,\%\, 209$ (d) $101^{-1} \,\%\, 256$

Theorem 3.6 (The Chinese Remainder Theorem)**.** If $\gcd(m, n) = 1$, then we have $a \equiv b \pmod{mn}$ if and only if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Proof. This is the statement of Theorem 1.6 translated into congruence notation. $\triangledown$

Definition. When $\gcd(m, n) = 1$, we say that m and n are *relatively prime* to each other. Three or more integers are *pairwise relatively prime* if they are relatively prime one to another.

Example. The numbers 8, 11, and 15 are pairwise relatively prime because $\gcd(8, 11)$, $\gcd(8, 15)$, and $\gcd(11, 15)$ all equal one.

Theorem 3.7. Suppose that $n_1, n_2, \ldots, n_k \in \mathbb{N}$ are pairwise relatively prime. Then the system of congruences $x \equiv c_i \pmod{n_i}$ has all its integer solutions $x \in [x_0]_N$, with

$$N = \prod_{i=1}^{k} n_i \quad \text{and} \quad x_0 = \sum_{i=1}^{k} c_i \left(\frac{N}{n_i}\right) \left(\frac{N}{n_i}\right)^{-1}$$

where each inverse represents any integer in the corresponding inverse class modulo n_i.

Proof. By design, we have $c_i(N/n_i)(N/n_i)^{-1} \equiv c_i \pmod{n_i}$ and $c_i(N/n_i)(N/n_i)^{-1} \equiv 0 \pmod{n_j}$ if $j \neq i$. This assures that x_0 is a solution. The Chinese remainder theorem then guarantees the uniqueness of the solution class modulo N. $\triangledown$

Example. Find all $x \in \mathbb{Z}$ satisfying both $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{9}$.
Solution. We have $N = 7 \times 9 = 63$ and $x_0 = 5(9)(9^{-1}) + 2(7)(7^{-1})$. Inverse mod computation gives $9^{-1} \equiv -3 \pmod{7}$ and $7^{-1} \equiv 4 \pmod{9}$. The particular solution $x_0 = 5(9)(-3) + 2(7)(4) = -79$ yields the general solution $x \in [-79]_{63} = [47]_{63}$.

Problem 25. Solve the system of linear congruences.
(a) $x \equiv 5 \pmod{16}$ and $x \equiv 1 \pmod{25}$
(b) $x \equiv 2 \pmod{9}$, $x \equiv 13 \pmod{10}$, $x \equiv 5 \pmod{11}$
(c) $x \equiv 6 \pmod{7}$, $x \equiv 10 \pmod{11}$, $x \equiv 12 \pmod{13}$
(d) $x \equiv 4 \pmod{5}$, $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{7}$

Theorem 3.8. If p is a prime number and $a^2 \equiv 1 \pmod{p}$, then $a \equiv \pm 1 \pmod{p}$.

Proof. If $p \mid a^2 - 1 = (a-1)(a+1)$, then by Theorem 2.3 we must have either $p \mid a - 1$, i.e., $a \equiv 1 \pmod{p}$, or $p \mid a + 1$, i.e., $a \equiv -1 \pmod{p}$. $\triangledown$

Problem 26. Prove that if $a^2 \equiv b^2 \pmod{p}$, then $a \equiv \pm b \pmod{p}$, where p is prime.

Theorem 3.9 (Wilson's Theorem)**.** If p is a prime number, then $(p-2)\,!\,\%\,p = 1$.

Proof. Let $S = \{1, 2, \ldots, p-1\}$. Theorem 3.5 implies that for each $a \in S$, there is a unique $a^{-1}\,\%\,p \in S$. Theorem 3.8 states that $a^{-1}\,\%\,p = a$ if and only if $a \in \{1, p-1\}$. Hence the subset $\{2, 3, \ldots, p-2\}$ consists of pairs of inverses modulo p, whose product satisfies the congruence $(p-2)\,! \equiv 1 \pmod{p}$. ▽

Example. With $p = 67$, Wilson's theorem states that $65\,!\,\%\,67 = 1$. Also, since $65\,! \equiv 1$ implies $64\,! \equiv 65^{-1} \pmod{67}$, we are able to get $64\,!\,\%\,67 = 33$. Hence, the theorem reduces the computational challenge involving large factorial mod a neighboring prime.

Problem 27. Use Wilson's theorem to help compute the mod operation.
(a) $100\,!\,\%\,101$ (b) $97\,!\,\%\,101$ (c) $310\,!\,\%\,313$ (d) $48\,!\,\%\,53$

Problem 28. Prove that a number $n \geq 2$ is prime if and only if $(n-1)\,! \equiv -1 \pmod{n}$.

4 Exponentiation

Example (Successive Squaring Algorithm). Evaluate $3^{47}\,\%\,100$.
Solution. First we express the exponent 47 as the sum of powers of two:

$$47 = 32 + 8 + 4 + 2 + 1 \quad \rightarrow \quad 3^{47} = 3^{32} \times 3^8 \times 3^4 \times 3^2 \times 3^1$$

Next we compute these powers mod 100 by successively squaring the previous power:

$$\begin{aligned} 3^2\,\%\,100 &= \ \ 9 \\ 3^4\,\%\,100 &= \ \ 9^2\,\%\,100 = 81 \\ 3^8\,\%\,100 &= 81^2\,\%\,100 = 61 \\ 3^{16}\,\%\,100 &= 61^2\,\%\,100 = 21 \\ 3^{32}\,\%\,100 &= 21^2\,\%\,100 = 41 \end{aligned}$$

Finally, $3^{47}\,\%\,100 = (41 \times 61 \times 81 \times 9 \times 3)\,\%\,100 = 5469687\,\%\,100 = 87$.

Problem 29. Use successive squaring algorithm to compute the power mod operation.
(a) $2^{33}\,\%\,11$ (b) $23^{99}\,\%\,20$ (c) $3^{59}\,\%\,79$. (d) $47^{250}\,\%\,100$

Definition. By a *complete residue system* modulo n, we mean a set of n integers from distinct residue classes modulo n.

Example. A complete residue system modulo 3 can be $\{0, 1, 2\}$, $\{1, 5, 9\}$, $\{-1, -2, -3\}$, or $\{11, 24, 43\}$. In general, $\{0, 1, \ldots, n-1\}$ is a complete residue system modulo n.

Theorem 4.1. Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then S is a complete residue system modulo n if and only if $\{ax \mid x \in S\}$ is also a complete residue system modulo n.

Proof. We must show that $x \not\equiv y \pmod{n}$ if and only if $ax \not\equiv ay \pmod{n}$ for all $x, y \in S$. Under the gcd condition, this follows right from Theorem 3.3. ▽

Example. Let $n = 5$ with $S = \{0, 1, 2, 3, 4\}$. Choose $a = 7$, where $\gcd(7, 5) = 1$. Then $7S = \{0, 7, 14, 21, 28\}$, whose remainders mod 5 correspond to $\{0, 2, 4, 1, 3\} = S$.

Theorem 4.2 (Fermat's Little Theorem)**.** Let p be a prime number and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$. In particular, if $p \nmid a$, then $a^{p-1} \,\%\, p = 1$.

Proof. Suppose that $p \nmid a$. Then $S = \{0, 1, \ldots, p-1\}$ and $T = \{ax \mid x \in S\}$ are both a complete residue system modulo p. In particular, the non-zero elements in T represent the classes of $1, 2, \ldots, p-1$. Hence,

$$a \times 2a \times \cdots \times (p-1)a \;\equiv\; 1 \times 2 \times \cdots \times (p-1) \pmod{p}$$

Theorem 3.3 allows us to cancel out all the common factors, so $a^{p-1} \equiv 1 \pmod{p}$, which is equivalent to $a^{p-1} \,\%\, p = 1$ and $a^p \equiv a \pmod{p}$. The latter congruence remains valid when $p \mid a$ as both sides belong to the zero class. ▽

Example. Prove that $35 \mid n^{13} - n$ for all $n \in \mathbb{Z}$.
Solution. By the Chinese remainder theorem, it suffices to show that $5 \mid n^{13} - n$ and $7 \mid n^{13} - n$. To avoid triviality, we assume $5 \nmid n$ and $7 \nmid n$. By Fermat's little theorem, $n^4 \equiv 1 \pmod{5}$, which implies $n^{12} \equiv 1^3 \pmod{5}$ and $n^{13} \equiv n \pmod{5}$. In a similar way, $n^6 \equiv 1 \pmod{7}$, which implies $n^{12} \equiv 1^2 \pmod{5}$ and $n^{13} \equiv n \pmod{5}$.

Problem 30. Prove that $77 \mid n^{31} - n$ for all $n \in \mathbb{Z}$.

Definition. Let $S = \{0, 1, \ldots, n-1\}$. The *Euler's phi function* $\phi(n)$ counts the number of elements in S which are relatively prime to n. Observe that this definition of $\phi(n)$ is unaffected if S is replaced by another complete residue system modulo n.

Example. We have $\phi(10) = 4$ and $\phi(11) = 10$.

Theorem 4.3. If p is a prime, then $\phi(p^k) = p^k - p^{k-1}$ for all $k \in \mathbb{N}$. In particular, $\phi(p) = p - 1$.

Proof. Let $n = p^k$ and $S = \{0, 1, \ldots, n-1\}$. By definition, $\phi(n) = n$ minus the number of elements $d \in S$ with $\gcd(d, n) > 1$. Since n has only one prime factor, $\gcd(d, n) > 1$ if and only if $p \mid d$, and the number of multiples of p in S is exactly $n/p = p^{k-1}$. ▽

Example. We have $\phi(313) = 313 - 1 = 312$ and $\phi(32) = 2^5 - 2^4 = 16$.

Problem 31. Evaluate the Euler's phi function.
(a) $\phi(81)$ (b) $\phi(101)$ (c) $\phi(625)$ (d) $\phi(1024)$

Problem 32. Prove that the number n is prime if and only if $\phi(n) = n - 1$.

Theorem 4.4. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. Let M, N, and MN be reduced residue systems modulo m, n, and mn, respectively. The theorem claims that $|MN| = |M \times N|$. If $x \in MN$, then x is relatively prime to mn, hence to m and n as well. Hence, there exists a unique pair $(c, d) \in M \times N$ such that $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$. Conversely, by Theorem 3.7, a pair of such congruences corresponds to a unique element $x \in MN$. Thus the pairing $x \iff (c, d)$ is a one-to-one correspondence between the two sets, which proves that $|MN| = |M \times N|$. ▽

Example. The last two theorems suffice for us to evaluate $\phi(n)$ for any $n \in \mathbb{N}$, e.g.,

$$792 = 2^3 \times 3^2 \times 11 \quad \to \quad \phi(792) = \phi(2^3) \times \phi(3^2) \times \phi(11)$$

and the result, $\phi(792) = (2^3 - 2^2) \times (3^2 - 3) \times (11 - 1) = 4 \times 6 \times 10 = 240$.

Problem 33. Evaluate the Euler's phi function.
(a) $\phi(360)$ (b) $\phi(\phi(81))$ (c) $\phi(4800)$ (d) $\phi(19392)$

Problem 34. Prove the propositions:
(a) If $n \geq 3$, then $\phi(n)$ is even.
(b) If n is odd, then $\phi(2n) = \phi(n)$.
(c) If n is even, then $\phi(2n) = 2\phi(n)$.

Problem 35. Prove that for all $n \in \mathbb{N}$, we have the formula

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product ranges over all the prime divisors of n, represented by p. Then use this to derive the identity $\phi(n^k) = n^{k-1}\phi(n)$ for all $k \in \mathbb{N}$.

Definition. By a *reduced residue system* modulo n, we mean a set of $\phi(n)$ integers from distinct residue classes $[a]_n$ for which $\gcd(a, n) = 1$.

Example. We can have $\{1, 2, 3, 4\}$ or $\{\pm 1, \pm 2\}$ for $n = 5$, or $\{1, 2, 4, 5, 7, 8\}$ if $n = 9$. Also, in general $\{1, 2, \ldots, p-1\}$ is a reduced residue system modulo a prime p.

Theorem 4.5. Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then S is a reduced residue system modulo n if and only if $\{ax \mid x \in S\}$ is also a reduced residue system modulo n.

Proof. In view of Theorem 4.1 and its proof, it suffices to show that $\gcd(x, n) = 1$ if and only if $\gcd(ax, n) = 1$, for all $x \in S$. But this is a consequence of the uniqueness of prime factorization, where $\gcd(a, n) = 1$ implies $\gcd(ax, n) = \gcd(x, n)$. ▽

Example. Let $n = 9$ and $S = \{1, 2, 4, 5, 7, 8\}$. Choose $a = 7$, where $\gcd(7, 9) = 1$. Then $7S = \{7, 14, 28, 35, 49, 56\}$, whose remainders mod 9 correspond to $\{7, 5, 1, 8, 4, 2\} = S$.

Theorem 4.6 (Euler's Theorem)**.** If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let $\gcd(a, n) = 1$. Theorem 5.7 allows us to have two reduced residue systems $S = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ and $\{ax \mid x \in S\}$. Hence,

$$r_1 \times r_2 \times \cdots \times r_{\phi(n)} \;\equiv\; ar_1 \times ar_2 \times \cdots \times ar_{\phi(n)} \pmod{n}$$

We cancel out the common factors by Theorem 3.3 and get $1 \equiv a^{\phi(n)} \pmod{n}$. ▽

Problem 36. Use Euler's theorem to compute the power mod operation.
(a) $7^{2699} \,\%\, 10$ (b) $7^{19392} \,\%\, 11$ (c) $5^{1234567} \,\%\, 18$ (d) $11^{123} \,\%\, 25$

Theorem 4.7. If both $\gcd(a, n) = 1$ and $\gcd(e, \phi(n)) = 1$, then the solution to the congruence $x^e \equiv a \pmod{n}$ is given by $x \in [a^d]_n$ for any positive integer $d \in [e^{-1}]_{\phi(n)}$.

Proof. We write $de = 1 + \phi(n)k$ for some $k \in \mathbb{Z}$, so that $x^{de} = x(x^{\phi(n)})^k$. Thus by Euler's theorem, $x^{de} \equiv x \pmod{n}$ for all $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$. This proves that $x^e \equiv a \pmod{n}$ is equivalent to $x \equiv a^d \pmod{n}$. ▽

Example. Solve the congruence $x^3 \equiv 9 \pmod{25}$.
Solution. We have $\phi(25) = 20$ and choose $d = 3^{-1} \,\%\, 20 = 7$, so $x \in [9^7]_{25} = [19]_{25}$.

Problem 37. Solve the congruence.
(a) $x^5 \equiv 2 (\text{mod } 13)$ (b) $x^7 \equiv 5 (\text{mod } 32)$ (c) $x^{17} \equiv 3 (\text{mod } 55)$ (d) $x^{39} \equiv 2 (\text{mod } 121)$

Example (The RSA Cryptosystem). Ali wants to send a secret number x (e.g., a credit card) to Beth over a non-secure internet connection. Beth sends first to Ali the integers e and $n > x$. Beth has obtained n as the product of two primes, i.e., $n = p \times q$, and no one but Beth knows p and q. Upon receiving e and n, Ali computes $x^e \,\%\, n = a$ (using successive squaring algorithm) and sends a to Beth. Meanwhile, Beth has computed $d = e^{-1} \,\%\, \phi(n)$ (extended euclidean algorithm) using her secret $\phi(pq) = (p-1)(q-1)$. After receiving a from Ali, Beth relies on Theorem 4.7 to retrieve the secret number, i.e., $a^d \,\%\, n = x$.

If a hacker intercepts e, n, and a, they will yet need p and q to discover the value of x. Hence, the RSA cryptosystem is only as secure as factoring n is hard. In fact, factoring takes exponential time with respect to digital length. For medium security, today's RSA implementation requires that n be around 1024 bits in size, i.e., of about 300 decimal digits.

Problem 38. Beth has chosen $p = 127$, $q = 79$, and $e = 17$.
(a) What numbers does Beth send to Ali?
(b) If Ali's secret number is $x = 2019$, what does he send to Beth?
(c) Help Beth compute her decryption key d.
(d) Verify that using d, Beth will retrieve Ali's secret number correctly.

Problem 39. Factor 11371 into two primes, assuming we know that $\phi(11371) = 11152$.

5 Primitive Roots

Definition. Let $\gcd(a, n) = 1$. The *order* of a *mod* n, denoted by $|a|_n$, is the smallest $k \in \mathbb{N}$ such that $a^k \,\%\, n = 1$. Observe that by definition, integers of the same residue class have the same order. Let us agree that whenever we have $|a|_n$, we also implicitly assume that $\gcd(a, n) = 1$, hence $|a|_n \leq \phi(n)$ by Euler's theorem.

Example. We have $|2|_7 = 3$, because $2^3 \,\%\, 7 = 1$ and $k = 3$ is the least positive exponent with such property. Also $|3|_7 = 6$.

Problem 40. Evaluate the order mod n.
(a) $|7|_{11}$ (b) $|7|_{12}$ (c) $|5|_{18}$ (d) $|2|_{25}$

Problem 41. Prove that $a^k \,\%\, n = 1$ for some $k \in \mathbb{N}$ if and only if $\gcd(a, n) = 1$.

Theorem 5.1. The following are some properties of order mod n.

1. If $a \equiv b \,(\text{mod}\, n)$, then $|a|_n = |b|_n$.
2. We have $a^k \,\%\, n = 1$ if and only if $|a|_n \mid k$.
3. The order of a divides phi, i.e., $|a|_n \mid \phi(n)$.
4. We have $a^j \equiv a^k \,(\text{mod}\, n)$ if and only if $j \equiv k \,(\text{mod}\, |a|_n)$.

Proof. In class. ▽

Problem 42. Prove the propositions:
(a) If $a \equiv b^{-1} \pmod{n}$, then $|a|_n = |b|_n$.
(b) If $\gcd(|a|_n, |b|_n) = 1$, then $|ab|_n = |a|_n \times |b|_n$.
(c) If $|a|_n = n - 1$ for some $a \in \mathbb{Z}$, then n is prime.

Theorem 5.2. For all $k \in \mathbb{N}$, we have

$$|a^k|_n = \frac{|a|_n}{\gcd(k, |a|_n)}$$

In particular, $|a^k|_n = |a|_n$ if and only if $\gcd(k, |a|_n) = 1$.

Proof. Let $m = |a|_n$ and $h = |a^k|_n$. We shall establish the equality $h = m/\gcd(k, m)$. First note that if d is any common divisor of k and m, then

$$(a^k)^{\frac{m}{d}} = (a^m)^{\frac{k}{d}} \equiv 1 \pmod{n}$$

so we know that $h \leq m/\gcd(k, m)$. Now the congruence $(a^k)^m = (a^m)^k \equiv 1 \pmod{n}$ implies that $h \mid m$ by Theorem 5.1. We write $ht = m$ for some $t \in \mathbb{N}$. Again by the same theorem, the congruence $(a^k)^h \equiv 1 \pmod{n}$ implies that $m \mid kh$. We write $ms = kh$ for some $s \in \mathbb{N}$. These two identities give $st = k$, so we have shown that $t \mid m$ and $t \mid k$. Hence, $t \leq \gcd(k, m)$ and $h = m/t \geq m/\gcd(k, m)$. ▽

Definition. When we have $|g|_n = \phi(n)$, we call g a *primitive root* modulo n.

Example. Find all the primitive roots modulo 7 and modulo 8.
Solution. Let $S = \{1, 2, 3, 4, 5, 6\}$, a reduced residue system modulo 7, where $\phi(7) = 6$. For each $a \in S$, we find that $|a|_7 = 6$ if and only if $a = 3$ or $a = 5$. Hence the primitive roots modulo 7 are given by the two classes $[3]_7$ and $[5]_7$. In a similar way, we find that modulo 8 has no primitive roots.

Problem 43. Find all the primitive roots modulo n.
(a) $n = 11$ (b) $n = 12$ (c) $n = 13$ (d) $n = 14$

Theorem 5.3. Suppose that $\gcd(g, n) = 1$. Then g is a primitive root modulo n if and only if the set $G = \{g^k \mid 1 \leq k \leq \phi(n)\}$ is a reduced residue system modulo n.

Proof. Let g be a primitive root. It is clear that $\gcd(g^k, n) = 1$. And if $g^j \equiv g^k \pmod{n}$ with $1 \leq k < j \leq \phi(n)$, then by Theorem 5.1, $\phi(n) \mid (j - k)$, which is not possible since $\phi(n) > j - k$. Hence, $g^j \not\equiv g^k \pmod{n}$ and G is a reduced residue system modulo n.

Conversely, let G be a reduced residue system. Since elements of G are distinct modulo n, and $g^{\phi(n)} \equiv 1 \pmod{n}$ by Euler's theorem, then $\phi(n)$ is the smallest exponent with this property, i.e., $|g|_n = \phi(n)$ and g is primitive root. ▽

Example. The primitive root 2 modulo 13 corresponds to the reduced residue system $\{2, 2^2, \ldots, 2^{12}\}$ verified in the below table.

k	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \,\%\, 13$	2	4	8	3	6	12	11	9	5	10	7	1

Now Theorem 5.2 says that $|2^k|_{13} = |2|_{13}$ if and only if $\gcd(k, 12) = 1$, i.e., $k = 1$, 5, 7, or 11. Hence, all the primitive roots modulo 13 are given by the classes $[2, 6, 11, 7]_{13}$.

Problem 44. Find all the primitive roots modulo 17, given that $g = 3$ is one of them.

Theorem 5.4. There are exactly $\phi(\phi(n))$ primitive root classes modulo n, if one exists.

Proof. Theorem 5.3 allows us to have a reduced residue system modulo n of the form $\{g^k \mid 1 \le k \le \phi(n)\}$, assuming that $|g|_n = \phi(n)$. Theorem 5.2 implies that $|g^k|_n = \phi(n)$ too if and only if $\gcd(k, \phi(n)) = 1$. In the range $1 \le k \le \phi(n)$, there are $\phi(\phi(n))$ such k and that many primitive roots. ▽

Problem 45. Determine the number of primitive root classes, assuming they exist.
(a) $n = 27$ (b) $n = 38$ (c) $n = 250$ (d) $n = 239$

Theorem 5.5. Primitive roots exist modulo any prime number p.

Proof. (1) The congruence $f(x) \equiv 0 \pmod p$ has at most $\deg f$ solution classes:

If $f(x) = ax + b$ with $p \nmid a$, then f has a unique zero class $[-ba^{-1}]_p$. By induction, let us assume the result for all $\deg f \le n-1$, and let $f(x)$ be a polynomial with leading term ax^n, again $p \nmid a$. If f has less than n zeros, then we are done; else let $r_1, r_2, \ldots, r_n$ be distinct zeros of $f(x)$ modulo p, and let

$$g(x) = f(x) - a(x - r_1)(x - r_2)\cdots(x - r_n)$$

Note that $\deg g < n$, and yet g has the same n zeros as f has. By induction hypothesis this is impossible unless $g(x)$ is the zero polynomial (mod p), i.e.,

$$f(x) \;\equiv\; a(x - r_1)(x - r_2)\cdots(x - r_n) \pmod p$$

And by Theorem 2.3, we have $f(x) \equiv 0 \pmod p$ if and only if $x \in [r_j]_p$ for $1 \le j \le n$.

(2) If $d \mid (p-1)$, then the congruence $x^d \equiv 1 \pmod p$ has exactly d solution classes:
Suppose $dk = p - 1$, so that we have the polynomial identity

$$x^{p-1} - 1 = (x^d - 1)\left((x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1\right)$$

By Fermat's little theorem, $x^{p-1} - 1$ has exactly $p-1$ zeros modulo p. Since p is prime, these zeros must come from those of the two polynomials on the right, the first of which has at most d, and the second at most $p - 1 - d$, according to (1). This is possible only if $x^d - 1$ has exactly d zeros (and the second one has exactly $p - 1 - d$ zeros).

(3) Write the prime factorization $p - 1 = \prod q_i^{e_i}$. By (2) there are exactly $q_1^{e_1}$ zeros of $x^{q_1^{e_1}} \equiv 1 \pmod p$, each of which has order a power of q_1, according to Theorem 5.1. Similarly, however, $q_1^{e_1-1}$ of these are also zeros of the congruence $x^{q_1^{e_1-1}} \equiv 1 \pmod p$, hence their orders are at most $q_1^{e_1-1}$. It follows that there exist $q_1^{e_1} - q_1^{e_1-1}$ integers of order $q_1^{e_1}$ and, by symmetry, of order $q_2^{e_2}$, $q_3^{e_3}, \ldots$ mod p. And since their orders are pairwise relatively prime, then the product of these integers (see Problem 42) has order $\prod q_i^{e_i} = p - 1$, i.e., a primitive root. ▽

Theorem 5.6 (The Primitive Root Theorem)**.** Primitive roots exist and only modulo 2, 4, p^k, or $2p^k$, where p is any odd prime and $k \in \mathbb{N}$.

Proof. Not here. ▽

Example (Discrete Logarithm Problem). According to Theorem 5.3, if g is a primitive root modulo n, then the congruence $g^x \equiv c \pmod{n}$ always has a solution for every $c \in \mathbb{Z}$ with $\gcd(c, n) = 1$. We employ this fact in solving the congruence $5^x \equiv 12 \pmod{13}$. First, we recall the primitive root 2 modulo 13:

k	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \,\%\, 13$	2	4	8	3	6	12	11	9	5	10	7	1

then we rewrite the congruence using powers of 2 and apply Theorem 5.1:

$$2^{9x} \equiv 2^6 \pmod{13} \quad \Longleftrightarrow \quad 9x \equiv 6 \pmod{12}$$

From here, we go back to Theorem 3.4 and work out the solution $x \in [2]_4$.

Problem 46. Solve the discrete logarithm problem.
(a) $10^x \equiv 3 (\mathrm{mod}\ 13)$ (b) $6^x \equiv -2 (\mathrm{mod}\ 13)$ (c) $13^x \equiv 3 (\mathrm{mod}\ 22)$ (d) $3^x \equiv 8 (\mathrm{mod}\ 23)$

Theorem 5.7. If g is a primitive root modulo a prime $p > 2$, then

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Proof. Let $\gcd(g, n) = 1$, so that $g^{p-1} \equiv 1 \pmod{p}$ by Euler's theorem. Moreover by Theorem 3.8, we also have $g^{(p-1)/2} \equiv \pm 1 \pmod{p}$. However, if $g^{(p-1)/2} \equiv 1 \pmod{p}$, then $|g|_p \leq (p-1)/2$ and g cannot be a primitive root, thus the claim. ▽

Problem 47. Prove the propositions, where p is any odd prime:
(a) The number 4 is not a primitive root modulo p.
(b) If $a \equiv x^2 \pmod{p}$ for any $x \in \mathbb{Z}$, then a is not a primitive root modulo p.
(c) If a, b are primitive roots modulo p, then ab is not a primitive root modulo p.

Problem 48. Find three odd primes modulo which 2 is not a primitive root.

6 Quadratic Residues

Example. Find all the solution classes of the quadratic congruence $x^2 \equiv 23 \pmod{77}$.
Solution. Since $77 = 7 \times 11$ with $\gcd(7, 11) = 1$, the problem is equivalent to solving the system $x^2 \equiv 23 \equiv 2 \pmod{7}$ and $x^2 \equiv 23 \equiv 1 \pmod{11}$. With prime modulus, each has two solution classes of the form $[\pm x]_p$, i.e., $x \equiv \pm 3 \pmod{7}$ and $x \equiv \pm 1 \pmod{11}$. Hence, we have four systems of linear congruences, and Theorem 3.7 gives the solutions $x \in [10, 32, 45, 67]_{77}$.

Problem 49. Solve the quadratic congruence.
(a) $x^2 \equiv 29 (\mathrm{mod}\ 35)$ (b) $x^2 \equiv 31 (\mathrm{mod}\ 55)$ (c) $x^2 \equiv 30 (\mathrm{mod}\ 91)$ (d) $x^2 \equiv 106 (\mathrm{mod}\ 119)$

Definition. Let $\gcd(a, n) = 1$. We call a a *quadratic residue* or *non-residue* modulo n, depending whether the congruence $x^2 \equiv a \pmod{n}$ has a solution or no solution, respectively. Observe that by definition, integers of the entire class $[a]_n$ are quadratic residues or non-residues as a is.

Example. Let $n = 9$ and $a \in S = \{1, 2, 4, 5, 7, 8\}$, reduced residue system. For each $x \in S$, we have $x^2 \in \{1, 4, 16, 25, 49, 64\}$, whose remainders mod 9 correspond to $\{1, 4, 7\}$. Hence, the congruence $x^2 \equiv a \pmod{n}$ has a solution if and only if $a \in [1, 4, 7]_9$. These are the quadratic residues mod 9, while the non-residues are given by $[2, 5, 8]_9$.

Problem 50. Find all the quadratic residues and non-residues mod n.
(a) 12 (b) 17 (c) 19 (d) 22

Definition. Let p be an odd prime, i.e., a prime $p > 2$, and let $a \in \mathbb{Z}$ such that $p \nmid a$. We define the *Legendre symbol* of a mod p to be

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

Observe that by definition, integers of the same residue class have the same Legendre symbol. Let us agree that whenever we write $\left(\frac{a}{p}\right)$, we assume that p is an odd prime and $p \nmid a$.

Example. Previously, we have $\left(\frac{1}{9}\right) = \left(\frac{4}{9}\right) = \left(\frac{7}{9}\right) = +1$ and $\left(\frac{2}{9}\right) = \left(\frac{5}{9}\right) = \left(\frac{8}{9}\right) = -1$.

Theorem 6.1 (Euler's Criterion)**.** The Legendre symbol satisfies the congruence

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

In particular, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. Suppose that $\left(\frac{a}{p}\right) = +1$. Then $a \equiv x^2 \pmod{p}$ for some $x \in \mathbb{Z}$. Note that $\gcd(x, p) = 1$, and so $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. Hence, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Now suppose that $\left(\frac{a}{p}\right) = -1$, and let g be a primitive root modulo p. By Theorem 5.3, $a \equiv g^k \pmod{p}$ for some $k \in \mathbb{N}$. Since a is a quadratic non-residue, it is necessary that k is odd, say $k = 2m + 1$. Then $a^{\frac{p-1}{2}} \equiv (g^{2m}g)^{\frac{p-1}{2}} = (g^{p-1})^m g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ by Theorem 5.7. Hence, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. ▽

Example. We have $\left(\frac{5}{13}\right) \equiv 5^6 \pmod{13}$. Since $15625 \equiv -1 \pmod{13}$, then $\left(\frac{5}{13}\right) = -1$.

Problem 51. Evaluate the Legendre symbol using Euler's criterion.
(a) $\left(\frac{3}{13}\right)$ (b) $\left(\frac{-3}{13}\right)$ (c) $\left(\frac{5}{17}\right)$ (d) $\left(\frac{15}{17}\right)$

Problem 52. Prove that if g is a primitive root modulo p, then $\left(\frac{g}{p}\right) = -1$.

Theorem 6.2. The Legendre symbol $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Proof. Euler's criterion gives $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. But since both sides are ± 1 and $p > 2$, then this congruence holds if and only if the two are equal. ▽

Problem 53. Prove that $\left(\frac{-1}{p}\right) = +1$ if and only if $p \,\%\, 4 = 1$.

Theorem 6.3 (Gauss' Lemma)**.** Let $d = \frac{p-1}{2}$ and $A = \{ak \mid 1 \le k \le d\}$. If n is the number of integers in $\{x \,\%\, p \mid x \in A\}$ which are larger than d, then $\left(\frac{a}{p}\right) = (-1)^n$.

Proof. Let $H = \{1, 2, \ldots, d\}$ and note that $\{\pm r \mid r \in H\}$ is a reduced residue system modulo p. By Theorem 4.1, elements in A are from distinct residue classes, hence n is the number of integers $x \in A$ for which $x \equiv -r \pmod{p}$ for some $r \in H$. Moreover observe that it is impossible to have $x, y \in A$ with $x \in [r]_p$ and $y \in [-r]_p$, because then $p \mid x + y = aj$, with $2 \le j \le 2d = p - 1$, and p divides neither a nor j. It follows that the d elements of A are congruent to those in H, except that n of them need a minus sign, i.e., $a \times 2a \times \cdots \times da \equiv (-1)^n \, 1 \times 2 \times \cdots \times d \pmod{p}$. We may divide both sides by $d!$ to obtain $a^d \equiv (-1)^n \pmod{p}$, and the result follows by Euler's criterion. ▽

Example. Consider $\left(\frac{5}{13}\right)$, where $A = \{5, 10, 15, 20, 25, 30\}$. Their remainders mod 13 correspond to $\{5, 10, 2, 7, 12, 4\}$. Three of these are larger than 6, so $\left(\frac{5}{13}\right) = (-1)^3 = -1$.

Problem 54. Repeat Problem 51 using Gauss' lemma.

Theorem 6.4 (Eisenstein's Lemma)**.** If a is odd, then

$$\left(\frac{a}{p}\right) = (-1)^m \quad \text{where} \quad m = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor$$

Proof. Our goal is to have $m \equiv n \pmod 2$, with the number n from Gauss' lemma, so then $(-1)^m = (-1)^n$. Now let $H = \{1, 2, \ldots, d = \frac{p-1}{2}\}$. In the proof of Gauss' lemma, the set $\{ak \mid k \in H\} \equiv \{\pm r \mid r \in H\} \pmod p$, with exactly n of them need the minus sign, i.e., where $ak \,\%\, p = p - r$. Since $ak = \lfloor ak/p \rfloor p + ak \,\%\, p$, we get the identity

$$\sum_{k=1}^{d} ak = \sum_{k=1}^{d} \left\lfloor \frac{ak}{p} \right\rfloor p + \sum_{i=1}^{n} (p - r_i) + \sum_{j=n+1}^{d} r_j$$

where $\{r_i \mid i \in H\} = H$, so we also have

$$\sum_{k=1}^{d} k = \sum_{i=1}^{n} r_i + \sum_{j=n+1}^{d} r_j$$

Subtracting this last equation from the one preceding will get us

$$(a-1)\sum_{k=1}^{d} k = \sum_{k=1}^{d} \left\lfloor \frac{ak}{p} \right\rfloor p + \sum_{i=1}^{n} p - 2\sum_{i=1}^{n} r_i$$

We now take remainder mod 2, where both $a \,\%\, 2 = 1$ and $p \,\%\, 2 = 1$, and conclude that $0 \equiv m + n - 0 \pmod 2$, i.e., that $m \equiv n \pmod 2$. ▽

Example. Consider $\left(\frac{5}{13}\right)$, where $d = 6$. Here $m = \lfloor \frac{5}{13} \rfloor + \lfloor \frac{10}{13} \rfloor + \lfloor \frac{15}{13} \rfloor + \lfloor \frac{20}{13} \rfloor + \lfloor \frac{25}{13} \rfloor + \lfloor \frac{30}{13} \rfloor = 0 + 0 + 1 + 1 + 1 + 2 = 5$. Hence, $\left(\frac{5}{13}\right) = (-1)^5 = -1$.

Problem 55. Repeat Problem 51 using Eisenstein's lemma.

Theorem 6.5. The Legendre symbol $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. In the last identity of the preceding proof, let $a = 2$ and note that $\lfloor 2k/p \rfloor = 0$ for all $k \in H$. Hence, we get $\sum_1^d k \equiv 0 + n - 0 \pmod 2$, implying that $(-1)^n = (-1)^{1+2+\cdots+d}$. But note that $1 + 2 + \cdots + \frac{p-1}{2} = \frac{p^2-1}{8}$, and that $(-1)^n = \left(\frac{2}{p}\right)$ by Gauss' lemma. ▽

Problem 56. Prove that $\left(\frac{2}{p}\right) = +1$ if and only if $p \equiv \pm 1 \pmod 8$.

Theorem 6.6 (The Quadratic Reciprocity Law)**.** If p and q are distinct odd primes, then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Proof. Let $P = \{x \mid 1 \le x \le \frac{p-1}{2}\}$ and $Q = \{y \mid 1 \le y \le \frac{q-1}{2}\}$. Then $P \times Q$ contains $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ elements which we bipartition into $S_1 = \{(x,y) \mid py < qx\}$ and $S_2 = \{(x,y) \mid qx < py\}$. (Note that $py = qx$ is not possible as $p \nmid qx$.) For each $x \in P$, we have $(x,y) \in S_1$ if and only if $1 \le y \le \lfloor qx/p \rfloor$, and similarly for S_2. Hence,

$$|S_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor \quad \text{and} \quad |S_2| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$$

So by Eisenstein's lemma, $(-1)^{|S_1|} = \left(\frac{q}{p}\right)$ and $(-1)^{|S_2|} = \left(\frac{p}{q}\right)$. Then with the fact that $|S_1| + |S_2| = |P \times Q|$, we conclude that $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$. ▽

Example. Consider $\left(\frac{792}{929}\right)$. Since $792 = 2^3 \times 3^2 \times 11$, we have $\left(\frac{792}{929}\right) = \left(\frac{2}{929}\right)\left(\frac{11}{929}\right)$. Then we evaluate separately, $\left(\frac{2}{929}\right) = (-1)^{107880} = +1$ and $\left(\frac{11}{929}\right) = \left(\frac{929}{11}\right)(-1)^{464\times 5} = \left(\frac{5}{11}\right) = \left(\frac{11}{5}\right)(-1)^{5\times 2} = \left(\frac{1}{5}\right) = +1$. The result, $\left(\frac{792}{929}\right) = (+1)(+1) = +1$.

Problem 57. Evaluate the Legendre symbol using reciprocity law.
(a) $\left(\frac{37}{83}\right)$ (b) $\left(\frac{71}{103}\right)$ (c) $\left(\frac{-69}{239}\right)$ (d) $\left(\frac{1414}{2063}\right)$

Problem 58. Prove that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if and only if either $p \,\%\, 4 = 1$ or $q \,\%\, 4 = 1$.

Definition. Let $P = p_1 \times p_2 \times \cdots \times p_k$ be the product of odd primes, not necessarily distinct, and let $\gcd(a, P) = 1$. We define the *Jacobi symbol* of a mod P to be

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \times \left(\frac{a}{p_2}\right) \times \cdots \times \left(\frac{a}{p_k}\right)$$

Hence, $\left(\frac{a}{P}\right) = \pm 1$ and is a generalization of the Legendre symbol, where $k = 1$. Observe that by definition, integers of the same residue class have the same Jacobi symbol. Let us agree that whenever we write $\left(\frac{a}{P}\right)$, we assume that $P \ge 3$ is odd and $\gcd(a, P) = 1$.

Theorem 6.7. The following are some properties of the Jacobi symbol.

1. $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$
2. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$
3. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$
4. $\left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right)(-1)^{\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)}$

where $Q \ge 3$ is another odd number relatively prime to P.

Proof. In class. ▽

Example. Although 35 is composite, we may treat the Legendre symbol $\left(\frac{35}{97}\right)$ as a Jacobi symbol, hence $\left(\frac{35}{97}\right) = \left(\frac{97}{35}\right)(-1)^{48\times 17} = \left(\frac{27}{35}\right) = \left(\frac{35}{27}\right)(-1)^{17\times 13} = -\left(\frac{8}{27}\right) = -\left(\frac{2}{27}\right) = -(-1)^{91} = +1$.

Problem 59. Redo Problem 57 using Jacobi symbol.

Problem 60. Prove that if the Jacobi symbol $\left(\frac{a}{P}\right) = -1$, then a is a quadratic non-residue modulo P.

1. (a) 3 (b) 21 (c) 26 (d) –15
2. (a) 9 (b) 2 (c) 21 (d) 0
3. Let $n = 2k + 1$ or $n = 2k$.
4. Follow example.
5. (a) 9 (b) 2 (c) 26 (d) 3
6. (a) 1 (b) 9 (c) 5 (d) 1
7. Theorem 1.5.
8. Follow example.
9. Follow example.
10. Theorem 1.7.
11. (a) $(-21+55k, 13-34k)$ (b) $\emptyset$ (c) $(-49+17k, 14-5k)$ (d) $(24+7k, 40+12k)$
12. Prove contrapositive.
13. (a) C (b) C (c) P (d) C
14. (a) 29 (b) 97 (c) 79 (d) 239
15. Theorem 2.3.
16. (a) 30 (b) 11 (c) 32 (d) 28
17. (a) 80 (b) 2 (c) 99225 (d) 303
18. 42,826,261
19. Theorem 3.1.
20. Theorem 1.4.
21. Theorem 1.6.
22. Follow definition.
23. (a) $[12]_{13}$ (b) $[3]_7$ (c) $[172]_{341}$ (d) $[64]_{97}$
24. (a) 19 (b) 35 (c) 31 (d) 109
25. (a) $[101]_{400}$ (b) $[533]_{990}$ (c) $[1000]_{1001}$ (d) $[269]_{420}$
26. Theorem 2.3.
27. (a) 100 (b) 17 (c) 156 (d) 11
28. Wilson's theorem.
29. (a) 8 (b) 7 (c) 47 (d) 49
30. Follow example.
31. (a) 54 (b) 100 (c) 500 (d) 512
32. Follow definition.
33. (a) 96 (b) 18 (c) 1280 (d) 6400
34. Factor n into primes.
35. Factor n into primes.
36. (a) 3 (b) 5 (c) 5 (d) 6
37. (a) $[6]_{13}$ (b) $[13]_{32}$ (c) $[38]_{55}$ (d) $[39]_{121}$
38. (a) 10033 and 17 (b) 4655 (c) 4625 (d) 2019
39. 83
40. (a) 10 (b) 2 (c) 6 (d) 20
41. Theorem 3.5.
42. Theorem 5.1.
43. (a) $[2, 6, 7, 8]_{11}$ (b) $\emptyset$ (c) $[2, 6, 7, 11]_{13}$ (d) $[3, 5]_{14}$
44. $[3, 5, 6, 7, 10, 11, 12, 14]_{17}$
45. (a) 6 (b) 6 (c) 40 (d) 96
46. (a) $[4]_6$ (b) $[11]_{12}$ (c) $[8]_{10}$ (d) $[10]_{11}$
47. Theorem 5.7
48. Many examples.
49. (a) $[8, 13, 22, 27]_{35}$ (b) $[14, 19, 36, 41]_{55}$ (c) $[11, 24, 67, 80]_{91}$ (d) $[15, 36, 83, 104]$
50. (a) $[1]_{12}$ (b) $[1, 2, 4, 8, 9, 13, 15, 16]_{17}$ (c) $[1, 4, 5, 6, 7, 9, 11, 16, 17]$ (d) $[1, 3, 5, 9, 15]$
51. (a) +1 (b) +1 (c) −1 (d) +1
52. Theorem 3.8 and Euler's criterion.
53. Let $p = 4k + 1$ or $p = 4k + 3$.
54. (a) +1 (b) +1 (c) −1 (d) +1
55. (a) +1 (b) +1 (c) −1 (d) +1
56. Let $p = 8k \pm 1$ or $p = 8k \pm 3$.
57. (a) +1 (b) −1 (c) +1 (d) +1
58. Let $p = 4k \pm 1$ and $q = 4h \pm 1$.
59. (a) +1 (b) −1 (c) +1 (d) +1
60. Follow definition.