
1.1 Divisibility

Let \( a, b \in \mathbb{Z} \), we say that \( a \) divides \( b \), and write \( a \mid b \) if there is an integer \( n \) such that \( b = an \).

Properties:

1. For every \( a \neq 0 \), \( a \mid 0 \) and \( a \mid a \). For every \( b \), \( \pm 1 \mid b \).
2. If \( a \mid b \) and \( b \mid c \), then \( a \mid c \).
3. If \( a \mid b \) and \( a \mid c \), then \( a \mid (xb + yc) \) for any \( x, y \in \mathbb{Z} \). In this case \( a \) is called a common divisor of \( b \) and \( c \).
4. If \( a \mid b \) and \( b \neq 0 \), then \( |a| \leq |b| \)

Notation 1.1 Let \( a, b, r \in \mathbb{Z} \)

1. \( a \equiv b \mod r \iff r \mid (a - b) \). This is an equivalence relation on \( \mathbb{Z} \).

1.2 Greatest common divisor (gcd) and the Euclidean algorithm

Proposition 1.2 Let \( a, b \in \mathbb{Z} \) not both zero. There is a unique \( d \in \mathbb{N} \) such that

1. \( d \mid a \) and \( d \mid b \) (so that \( d \) is a common factor of \( a \) and \( b \))
2. if \( d_1 \) is any common factor of \( a \) and \( b \), then \( d_1 \mid d \)

We call this integer \( d \) the greatest common divisor, or gcd of \( a \) and \( b \). We denote this by \( (a, b) \) or \( \gcd(a, b) \).

The proof of the above is also a procedure to find \( \gcd(a, b) \). This is called the Euclidean algorithm. We assume \( a, b \) are positive integers.

We will write

\[ x \% y = x \mod y = \text{remainder of } x \text{ after dividing by } y \]

Assume \( a > b \), let \( r_{-1} := a \) and \( r_0 := b \). Recursively define

\[ r_{j-1} = r_j q_{j+1} + r_{j+1} \]  \hspace{1cm} (1)

where \( r_{j+1} = r_{j-1} \mod r_j \) (with \( 0 \leq r_{j+1} < r_j \)). If \( r_n = 0 \) then \( \gcd(a, b) = r_{n-1} \).
def euclid(a,b):
    if a > b:
        q = a
        r = b
    else:
        r = a
        q = b
    while q >= r:
        print (q,r)
        if r == 0:
            return q
        else:
            q_ = r
            r_ = q % r
            r = r_
            q = q_

Proof:  First we show that the algorithm terminates. Since $0 \leq r_{j+1} < r_j$
for all $j$. We must have $r_n = 0$ for some $n$.

Next we show that $r_{n-1} \mid a$ and $r_{n-1} \mid b$. Clearly $r_{n-1} \mid r_{n-2}$. Suppose
$r_j \mid r_{j-1}$. By definition $r_{j-1} = r_j m$ for some $m \in \mathbb{Z}$. Putting this in the
equation $r_{j-2} = r_{j-1}q_j + r_j$ gives

$$r_{j-2} = r_{j-1}(q_j + m)$$

Hence $r_{j-1} \mid r_{j-2}$. Repeating the argument $n$ times shows that this is true
for $j = 0, \ldots, n$. In particular, $r_{n-1} \mid a$ and $r_{n-1} \mid b$.

Finally, to show that $\gcd(a, b) = r_{n-1}$, suppose $d'$ is a common factor of
$r_{-1} = a$ and $r_0 = b$. By (1), if $d' \mid r_{j-1}$ and $d' \mid r_j$, then $d' \mid r_{j+1}$. Since $d'$
is a common factor of $a$ and $b$, certainly $d' \mid r_{-1}$ and $d' \mid r_0$. Repeating this
argument $n - 1$ times shows that $d' \mid r_{n-1}$. \hfill \square

Note 1.3  The greatest common divisor can be defined for arbitrary sets of integers.

To compute this, let $d_1 = \gcd(a_1, a_2)$, then $\gcd(a_1, \ldots, a_n) = \gcd(d_1, a_3, \ldots, a_n)$
and repeat.

Fact: let $S \subset \mathbb{Z}$, then there exists a finite subset $S' \subset S$ such that $\gcd(S) = \gcd(S')$.

Example 1.4  Find the greatest common divisor of 39 and 24.

$$39 = 24 \times 1 + 15$$
\[24 = 15 \times 1 + 9\]
\[15 = 9 \times 1 + 6\]
\[9 = 6 \times 1 + 3\]
\[6 = 3 \times 2 + 0\]

so gcd(39, 24) = 3.

**Example 1.5** Find the greatest common divisor of 54, 60, and 42. First find gcd(54, 60)

\[60 = 54 \times 1 + 6\]
\[54 = 6 \times 9 + 0\]

so gcd(54, 60) = 6. Now 6 divides 42, so gcd(54, 60, 42) = 6.

**Definition 1.6** We say that \(a, b \in \mathbb{Z}\) are coprime if gcd\((a, b) = 1\).

**1.3 The Extended Euclidean Algorithm**

**Proposition 1.7** Let \(a, b \in \mathbb{Z}\) and \(d = \text{gcd}(a, b)\). There exist integers \(x, y\) such that

\[d = ax + by.\]

The proof of this also follows from the Euclidean algorithm. Recall that for \(a := r_{-1} > b := r_0\), the Euclidean algorithm generates a sequence \(q_1, \ldots, q_n\) by the following equations

\[r_{j-1} = r_j q_{j+1} + r_{j+1}\]

where \(\text{gcd}(a, b) = r_n\).

```python
l_ = [q_n,..,q_1]
def backsub(l_):
    result = [-l[0],1]
    for i in l[1:]:
        a = result[1]-result[0]*i
        b = result[0]
        result = [a,b]
    print a,b
    return result
```

3
Example 1.8 Find integers $a, b$ such that $28a + 15b = \gcd(28, 15)$.

$$
28 = 15 \times 1 + 13 \\
15 = 13 \times 1 + 2 \\
13 = 2 \times 6 + 1 \\
1 = -6 \times 2 + 13 \\
= 13 \times 7 - 6 \times 15 \\
= 28 \times 7 + 15 \times (-13)
$$

1.4 Exercises

1. Let $m$ be a nonzero integer. Prove that $a \mid b$ if and only if $ma \mid mb$.

Solution: Suppose that $a \mid b$. Then there is an integer $k$ such that $b = ka$. Multiplying both sides by $m$ gives $mb = k(ma)$, so $ma \mid mb$. Conversely, suppose that $ma \mid mb$, then there is an integer $k$ such that $mb = kma$. So $m(b-ka) = 0$, since $m \neq 0$, we must have $b = ka$. Hence $a \mid b$.

2. Prove that $\gcd(ma, mb) = m \gcd(a, b)$ for any $m, a, b \in \mathbb{Z}$.

Solution: Let $d = \gcd(a, b)$. Then $md \mid ma$ and $md \mid mb$. Suppose $x \mid ma$ and $x \mid mb$. We show that $x \mid md$. Let $x_1 = \gcd(m, x)$, and write $x = x_1x'$, $m = x_1m'$. Then $kx = ma$ for some integer $k$. This gives $kx' = m'a$. Since $x'$ does not divide $m'$, we must have $x' \nmid a$. Similarly $x' \mid b$. Hence $x' \mid d$, so $x \mid md$.

Alternatively, we can use the Euclidean algorithm. Suppose

$$
r_{j-1} = r_jq_{j+1} + r_{j+1}
$$

terminates with $\gcd(a, b) = r_n$. Then we can multiply each equation by $m$ to get

$$
(mr_{j-1}) = (mr_j)q_{j+1} + (mr_{j+1})
$$

which terminates at $mr_n = m \gcd(a, b)$. This is exactly the same sequence of equations if we start with $r'_{j-1} = ma$ and $r'_{j+1} = mb$, so $\gcd(ma, mb) = m \gcd(a, b)$. 
3. Prove that if \( \gcd(a, m) = \gcd(b, m) = 1 \), then \( \gcd(ab, m) = 1 \).

Solution: Let \( x \) be an integer such that \( x \mid ab \) and \( x \mid m \). Let \( x_1 = \gcd(x, a) \). Write \( x = x_1 x' \) and \( a = x_1 a' \). Then \( a'b = kx' \). Since \( x' \) does not divide \( a' \), we must have \( x' \) divides \( b \). Now \( x' \mid x \) and \( x \mid m \) so \( x' \mid m \). This shows that \( x' \mid \gcd(b, m) \), so \( x' = 1 \). Similarly, \( x_1 \mid a \) and \( x_1 \mid m \), so \( x_1 \mid \gcd(a, m) \). Thus \( x_1 = 1 \). This shows that \( x = x_1 x' = 1 \). Hence \( \gcd(ab, m) = 1 \).

4. Prove that if \( n \) is odd, then \( n^2 - 1 \) is divisible by 8.

Solution: Let \( n = 2m + 1 \), then \( (2m + 1)^2 - 1 = 4m^2 + 4m = 4m(m + 1) \). Since \( 2 \mid m(m + 1) \), we see that \( 8 \mid n^2 - 1 \).

5. Find \( d = \gcd(1819, 3587) \) and integers \( x, y \) such that

\[
\begin{align*}
d &= 1819x + 3587y.
\end{align*}
\]

Solution: Using the Euclidean algorithm, we have

\[
\begin{align*}
3587 &= 1819 \times 1 + 1768 \\
1819 &= 1768 \times 1 + 51 \\
1768 &= 51 \times 34 + 34 \\
51 &= 34 \times 1 + 17
\end{align*}
\]

so \( d = 17 \). Backsubstituting gives \( 71 \cdot 1819 - 36 \cdot 3587 = 17 \).

6. Find integers \( a, b \) such that \( 1132a + 332b = \gcd(1132, 332) \).

Solution: Using the Euclidean algorithm, we have

\[
\begin{align*}
1132 &= 332 \times 3 + 136 \\
332 &= 136 \times 2 + 60 \\
136 &= 60 \times 2 + 16 \\
60 &= 16 \times 3 + 12 \\
16 &= 12 \times 1 + 4
\end{align*}
\]

so \( d = 4 \). Backsubstituting gives \( 22 \cdot 1132 - 75 \cdot 332 = 4 \).

7. Let \( f(n) = 10^n + 3 \cdot 4^{n+2} + 5 \). Show that \( f(n)/9 \in \mathbb{Z} \) for all for all positive integers \( n \).

Solution: We do this by induction. The statement is true for \( n = 1 \), since \( f(1) = 297 = 9 \times 33 \). Assume it is true for \( n \), then

\[
\begin{align*}
f(n + 1) &= 10^{n+1} + 3 \cdot 4^{n+3} + 5
\end{align*}
\]
\[
\begin{align*}
= & \quad 10 \cdot 10^n + 12 \cdot 4^{n+2} + 5 \\
= & \quad 10 \cdot f(n) - 9 \cdot 5 - 18 \cdot 4^{n+2}
\end{align*}
\]

By the induction hypothesis \(9 \mid f(n)\) so \(9 \mid f(n+1)\). Hence \(9 \mid f(n)\) for all positive integers \(n\).

8. The least common multiple of \(a, b\) is defined as an integer \(m\) satisfying the following conditions

Let \(a, b\) be positive integers and suppose \(m\) is a positive integer satisfying the following conditions

(a) \(a \mid m\) and \(b \mid m\)
(b) for all \(m'\) with \(a \mid m'\) and \(b \mid m'\) we have \(m \mid m'\)

Show that \(m\) is unique. We denote \(m = \text{lcm}(a, b)\), called the least common multiple of \(a\) and \(b\). Show that \(\text{lcm}(a, b) = ab / \gcd(a, b)\).

**Solution:** Let \(m\) and \(n\) be two integers satisfying the properties above. Then by property 2, we have \(m \mid n\) and \(n \mid m\) so \(m = n\).

Let \(d = \gcd(a, b)\). Clearly \(a, b\) both divide \(ab / d\). Since we can write this as \(a(b / d) = (a / d)b\). Suppose \(a \mid m'\) and \(b \mid m'\). Then \((a / d) \mid m'\) and \(\gcd(a / d, b) = 1\) so \((a / d)b \mid m'\). By uniqueness of lcm, we have \(\text{lcm}(a, b) = m'\).

9. Show that \(f(n) = n^4 + 2n^3 + 2n^2 + 2n + 1\) is not a perfect square for any \(n \in \mathbb{N}\).

**Solution:** We factorise \(f(n) = (n^2 + 1)^2 + 2n(n^2 + 1) = (n^2 + 1)(n^2 + 2n + 1) = (n^2 + 1)(n + 1)^2\). Since \(n^2 + 1\) is not a perfect square, neither is \(f(n)\).

2 Primes in \(\mathbb{Z}\)

2.1 Infinitude of primes

Let \(p \in \mathbb{Z}\) we say that \(p\) is prime if \(p\) is not equal to 1 and \(p\) has no factors other than 1 or itself, i.e. if \(a \mid p\) and \(a > 0\), then \(a = 1\) or \(p\). If \(p\) is not prime or 1, it is called composite.

**Theorem 2.1** There are infinitely many primes in \(\mathbb{Z}\).
Proof: This goes back to Euclid. Suppose there are finitely many primes \( p_1, \ldots, p_n \). Let \( n = p_1 \cdots p_n \) be the product of all the primes. Let \( p \) be a prime dividing \( n \). Now \( p \) cannot be any of the \( p_1, \ldots, p_n \), since the remainder of \( n \) when divided by \( p_i \) is equal to 1. Hence \( p \) is a prime not in the original finite list \( \{p_1, \ldots, p_n\} \), which is a contradiction. \( \square \)

2.2 Unique factorisation in \( \mathbb{Z} \)

Proposition 2.2 Every integer \( a > 1 \) can be written as a product of primes.

Proof: First we show that any integer \( a > 1 \) can be factored into primes. We proceed by induction, suppose any integer less than \( a \) can be factored into primes. If \( a \) is prime, then it is its own prime factorisation. If not, \( a = bc \) where \( 1 < b, c < a \). By induction hypothesis \( b, c \) can be factored into primes, hence \( a \) can be as well. \( \square \)

Theorem 2.3 Every \( a \in \mathbb{Z} \) can be factorised as \( \pm p_1^{e_1} \cdots p_n^{e_n} \) where \( p_1, \ldots, p_n \) are primes. Furthermore, this factorisation is unique up to permutation of \( \{p_1, \ldots, p_n\} \).

To show uniqueness, we need the following lemma.

Lemma 2.4 If \( a \mid bc \) and \( \gcd(a, b) = 1 \) then \( a \mid c \). Consequently, if \( p \mid p_1 \cdots p_n \) and each \( p, p_i \) are prime then \( p \mid p_i \) for some \( i \).

Proof: Homework. \( \square \)

Proof: (of Theorem 2.3) Let \( a = p_1 \cdots p_n \) and \( a = q_1 \cdots q_m \) be two prime factorisations of \( a \). Let \( p \) be a prime divisor of \( a \). By Lemma 2.4 we must have (after appropriate relabelling) \( p = p_1 \) and \( p = q_1 \). Repeat the argument on \( ap^{-1} \) to see that \( p_2 = q_2 \). Continuing in this fashion shows that \( m = n \) and \( p_i = q_i \) for all \( i = 1, \ldots, n \). \( \square \)

The prime numbers are building blocks for other numbers. We can ask the following basic questions

- Given \( n \in \mathbb{N} \) how do we determine (efficiently) whether \( n \) is prime? (trial division, primality testing)
- Given that we have found \( k \) prime numbers \( p_1, \ldots, p_k \), how do we find the next prime?
• Are there formulas which generate prime numbers? (prime generating polynomials, special types of primes e.g. Mersenne primes, Fermat primes)

• How many primes are there less than \( N \)? More generally, let \( \pi(N) \) = number of primes between 0 and \( N \). What does the function \( \pi \) look like?

• How do we find all the prime numbers less than \( N \)? (Sieve)

We have good answers to only some of these questions.

### 2.3 Prime seives

The Sieve of Eratosthenes

### 2.4 Special primes

One way of constructing primes is to consider the number \( a^n - 1 \). We can factorise this as \( a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + 1) \), so a necessary condition for \( a^n - 1 \) to be prime is \( a = 2 \) and \( n \) is prime.

If \( p \) is prime, is \( 2^p - 1 \) also prime? No: \( 2^{11} - 1 = 23 \times 89 \).

**Definition 2.5** A Mersenne prime is a prime number of the form \( 2^p - 1 \).

It is not known if there are infinitely many Mersenne primes.

According to Wikipedia, the largest known prime number is a Mersenne prime: \( 2^{57,885,161} - 1 \). In fact, the ten largest known primes are Mersenne primes. This is the 48th Mersenne prime known. Since 1997, all new Mersenne primes have been found by a distributed computing project known as the Great Internet Mersenne Prime Search.

Let \( n \in \mathbb{N} \). We say that \( n \) is **perfect** if \( n \) is equal to the sum of its proper divisors, or equivalently, if the sum of all the divisors of \( n \) is equal to \( 2n \).

Let \( \sigma(n) \) = sum of all divisors of \( n \), then \( n \) is perfect if \( \sigma(n) = 2n \).

There is a close relationship between perfect numbers and Mersenne primes.

**Theorem 2.6** *(Euclid-Euler)* Let \( n \) be a positive even integer. Then \( n \) is perfect if and only if \( n = 2^{p-1}(2^p - 1) \) for some prime \( p \) with \( 2^p - 1 \) prime.
Proof: Suppose $2^p - 1$ is prime and let $n = 2^{p-1}(2^p - 1)$. Then

$$
\sigma(n) = \sigma(2^{p-1}(2^p - 1)) = (1 + 2 + 2^2 + \cdots + 2^{p-1})(2^p - 1 + 1) = (2^p - 1)(2^p) = 2n
$$

so $n$ is perfect.

Suppose $n$ is an even perfect number. Then write $n = 2^j m$ where $m$ is odd. Then we can calculate the divisor sum of $n$ as follows

$$
\sigma(n) = (1 + 2 + \cdots + 2^j) \sigma(m) = (2^{j+1} - 1) \sigma(m).
$$

Since $n$ is perfect, we have $\sigma(n) = 2n$, so

$$
2^{j+1} m = (2^{j+1} - 1) \sigma(m).
$$

Since $2^{j+1} - 1$ does not divide $2^{j+1}$, it must divide $m$. Write $m = (2^{j+1} - 1)x$ for some $x \in \mathbb{N}$. Then

$$
\sigma(m) = 2^{j+1} x.
$$

If $x > 1$, then $1, x, m$ are distinct divisors of $m$

$$
2^{j+1} x = \sigma(m) \geq 1 + x + m = 1 + 2^{j+1} x
$$

which is a contradiction. Therefore $x = 1$, in which case $\sigma(m) = 2^{j+1} = (2^{j+1} - 1) + 1$. So $m = 2^{j+1} - 1$ is prime, and $n = 2^j (2^{j+1} - 1)$. Note that since $m$ is prime, $j + 1$ is necessarily prime as well. This proves the theorem. □

All known perfect numbers are even. It is not known whether odd perfect numbers exist.

Another way of cooking up primes would be to consider numbers of the form $a^n + 1$. Note that if $n = 2m + 1$ is odd, then $a^{2m+1} + 1 = (a + 1)(a^{2m} - a^{2m-1} + \cdots - a + 1)$ so it is composite for all $a > 1$. In fact, the same is true if $n$ has an odd divisor. Therefore, if $a^n + 1$ is prime, then $n = 2^r$ for some $r > 0$.

Note: not all such numbers are prime: $2^{2^5} + 1 = 641 \times 6700417$.

**Definition 2.7** A Fermat prime (resp. generalised Fermat prime) is a prime number of the form $2^{2^n} + 1$ (resp. $a^{2^n} + 1$).
The largest known Fermat prime is $2^{2^4} + 1$.

**Theorem 2.8** (Euler) Every factor of $2^{2^n} + 1$ is of the form $k2^{n+1} + 1$.

(Lucas) Every factor of $2^{2^n} + 1$ is of the form $k2^{n+2} + 1$.

**Proof:** We can’t prove this theorem now, but we can by the end of the course. See §6.2.

\[ \square \]

### 3 Modular arithmetic

Let $a, b, n \in \mathbb{Z}$. We write $a \equiv b \mod n$ if $n \mid (a - b)$. In other words, $a$ is equivalent to $b$ modulo $n$ if they have the same remainders after dividing by $n$.

Modular arithmetic works in much the same way as ordinary arithmetic.

**Lemma 3.1** If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.

**Proof:** We have $(a + c) - (b + d) = (a - b) + (c - d)$. Since $n$ divides $a - b$ and $c - d$, $n$ divides their sum. This shows that $a + c \equiv b + d \mod n$.

We have $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$. Same argument.

\[ \square \]

**Theorem 3.2** (Fundamental property) Let $f \in \mathbb{Z}[x]$ and $a \equiv b \mod n$. Then $f(a) \equiv f(b) \mod n$.

**Proof:** This follows by induction on $\deg(f)$ from Lemma 3.1. If $\deg(f) = 0$, this is clear. Assume $f(a) \equiv f(b) \mod n$ for all $f \in \mathbb{Z}[x]$ with $\deg(f) < n$. Then given $g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, using Lemma 3.1 and the induction hypothesis we have

$$a(a_n a_n^{-1}a_{n-1} + \cdots + a_1) \equiv b(b_n b_n^{-1}a_{n-1} + \cdots + a_1) \mod n$$

Adding $a_0$ to both sides give $g(a) \equiv g(b) \mod n$. This proves the theorem.

\[ \square \]

**Proposition 3.3** If $ka \equiv kb \mod n$ and $\gcd(k, n) = d$, then $a \equiv b \mod (n/d)$.
Proof: Since \( n \mid k(a - b) \) we have \( k(a - b) = nr \) for some \( r \in \mathbb{Z} \). Since \( \gcd(k, n) = d \), we can divide this equation by \( d \) to get

\[
\frac{k}{d} (a - b) = \left( \frac{n}{d} \right) r
\]

with \( k/d, n/d \in \mathbb{Z} \) and \( \gcd(k/d, n/d) = 1 \). By Lemma 2.4, \( n/d \) must divide \( (a - b) \), which proves the theorem. \( \square \)

Corollary 3.4 If \( p \) is prime, and \( ka \equiv kb \mod p \). Then \( a \equiv b \mod p \).

We can’t necessarily divide numbers modulo \( n \).

Example 3.5 There exists no integer \( a \) such that \( 2a \equiv 1 \mod 6 \). The proof is easy, suppose this holds, then multiplying the congruence by 3 gives \( 6a \equiv 0 \equiv 3 \) which is impossible. In general, if \( d = \gcd(b, n) \neq 1 \) then \( bx \equiv 1 \mod n \) has no solution in \( x \). Prove this!

Definition 3.6 Let \( a \) be an integer such that \( 0 < a < p \). We say that \( a \) is a unit modulo \( p \) if there exists \( 0 < b < p \) such that \( ab \equiv 1 \mod p \). We call \( b \) the inverse of \( a \) modulo \( p \).

We will return to this in the next section

3.1 Examples

Proposition 3.7 An integer \( a \in \mathbb{Z} \) is divisible by 9 if and only if the sum of its digits is also divisible by 9. (The same thing works for 3).

Proof: Let \( a \in \mathbb{Z} \). Write \( a \) in base 10 as follows \( a = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 \). By the rules of modular arithmetic, we have \( 10^n \equiv 1^n \equiv 1 \mod 9 \). Therefore

\[
a \equiv a_0 + \cdots + a_n \mod 9.
\]

In other words, the remainder when \( a \) is divided by 9 is the same as the remainder when the sum of its digits is divided by 9. This proves the proposition. \( \square \)

Proposition 3.8 Let \( a \in \mathbb{Z} \). If \( a \equiv 3 \mod 4 \), then \( a \) is not a sum of two squares.
Proof: We argue by contradiction. Suppose \( a = x^2 + y^2 \) for some \( x, y \in \mathbb{Z} \). Note that \( x^2 \equiv 0, 1 \mod 4 \) (just list the possibilities), therefore \( a \) is not congruent to 3 mod 4.

3.2 Linear congruences

In this subsection, we aim to provide a method to solve the linear congruence in one variable \( x \)

\[
ax \equiv b \mod n
\]  

(2)

where \( a, b, n \in \mathbb{Z} \).

To solve these congruences, we use the extended Euclidean algorithm. The linear congruence (2) can be rewritten as an ordinary equation

\[
ax + ny = b
\]

where \( y \in \mathbb{Z} \). Let \( d = \gcd(a, n) \), then a necessary condition for the equation to have solutions is that \( d \mid b \).

Assume that \( d \mid b \), then we can divide by \( d \) to get the equation

\[
a'x + n'y = b'
\]

where \( da' = a, dn' = n \) and \( db' = b \). Now \( (a', n') = 1 \), so by extended Euclidean algorithm, there are unique integers \( x', y' \) such that

\[
a'x' + n'y' = 1
\]

Multiplying by \( db' \) gives

\[
\begin{align*}
d(a'x'b') + d(n'y'b') &= db' \\
a(x'b') + n(y'b') &= b
\end{align*}
\]

so a solution is \( x = x'b' \). But \( x'b' + kn' \) are distinct solutions modulo \( n \) for any \( k = 0, \ldots, d - 1 \). Therefore we have found \( d \) solutions.

This (almost) proves the following Theorem, and provides a recipe to solve linear congruences.

**Theorem 3.9** The above congruence has solutions if and only if \( \gcd(a, n) \mid b \). If this holds, then there are \( \gcd(a, n) \) solutions modulo \( n \).
Proof: We showed that if \( d = \gcd(a, n) \) does not divide \( b \), then there are no solutions. The solution method by extended Euclidean algorithm given above find \( d \) solutions if \( d \mid b \), so there are at least \( d \) solutions modulo \( n \).

By Proposition 3.3, there are at most \( d \) solutions modulo \( n \). Indeed, any two solutions \( x_1, x_2 \) of the linear congruence \( ax \equiv b \mod n \) satisfy \( ax_1 \equiv ax_2 \mod n \), so by Proposition 3.3 must be congruent modulo \( n / \gcd(a, n) \). There are exactly \( \gcd(a, n) \) of these modulo \( n \). \( \square \)

Corollary 3.10 Let \( n \in \mathbb{N} \) and \( a \) be an integer such that \( 0 < a < n \). Then \( a \) has an inverse modulo \( n \) if and only if \( \gcd(a, n) = 1 \).

Proof: Put \( b = 1 \), then \( a \) has an inverse if and only if the solution \( ax \equiv 1 \mod n \) has a solution. By the above theorem, this occurs if and only if \( \gcd(a, n) | 1 \), i.e. \( \gcd(a, n) = 1 \). \( \square \)

Example 3.11 Solve the following linear congruence

\[
15x \equiv 12 \mod 21.
\]

We use the extended Euclidean algorithm to solve the above. First let \( r_{-1} = 21, r_0 = 15 \). Then

\[
\begin{align*}
21 &= 15 \times 1 + 6 \\
15 &= 6 \times 2 + 3 \\
6 &= 3 \times 2
\end{align*}
\]

Therefore \( \gcd(21, 15) = 3 \). Backsubstituting gives

\[
\begin{align*}
3 &= 15 - 6 \times 2 \\
&= 15 - (21 - 15) \times 2 \\
&= 3 \times 15 - 2 \times 21.
\end{align*}
\]

Multiply this by 4 to get \( 15 \times 12 - 21 \times 8 = 12 \). Therefore \( x \equiv 12, 19, 26 \mod 21 \) are solutions.

Later, we will see that we can use Euler’s strengthening of Fermat’s little theorem to do the following: there exists some \( r \) such that \( a^r \equiv 1 \mod n \), provided that \( \gcd(a, n) = 1 \).
3.3 The Chinese remainder theorem

The next natural class of problems to consider is simultaneous linear congruences. The statement of this theorem goes back to Sun Tzu, who is a Chinese mathematician/philosopher from 3rd or 5th century CE. The general problem can be stated

\[ a_i x \equiv b_i \mod n_i \]

where \(a_i, b_i, n_i\) for \(i = 1, \ldots, r\) are integers. Clearly a necessary condition for these congruences to have a common solution is for each congruence to be solvable. So we assume that \(\gcd(a_i, b_i) | n_i\), and that we have solve each congruence separately. This reduces the problem to

\[ x \equiv c_i \mod n_i \]  \hspace{1cm} (3)

where \(i = 1, \ldots, r\). The first form of the Chinese remainder theorem solves the case where \(n_1, \ldots, n_r\) are pairwise coprime

**Theorem 3.12** The system of congruences (3) has a unique solution modulo \(n_1 \cdots n_r\) if and only if \(\gcd(n_i, n_j) = 1\) for all \(i \neq j\).

**Proof:** Suppose that \(\gcd(n_i, n_j) = 1\) for all \(i \neq j\). This means there exists integers \(m_{ij}\) such that \(m_{ij} n_j \equiv 1 \mod n_i\) for all \(i, j = 1, \ldots, r\). Moreover \(m_{ij}\) is unique modulo \(n_i\). We can use this to produce a solution to (3) namely

\[ x = \sum_{i=1}^{r} c_i \prod_{j \neq i} m_{ij} n_j. \]

If \(x'\) is another solution to (3), then \(x - x' \equiv 0 \mod n_j\) for all \(j = 1, \ldots, r\). Since the \(n_1, \ldots, n_r\) are pairwise coprime, we must have \(x - x' \equiv 0 \mod n_1 \cdots n_r\).

Suppose that \(\gcd(n_1, n_2) \neq 1\), and (3) has a solution, say \(x\). Then \(x + n'\) where \(n' = n_1 \cdots n_r / \gcd(n_1, n_2)\) is another solution of (3) which is different from \(x\) modulo \(n_1 \cdots n_r\). This proves the theorem. \(\square\)

The above proof is constructive, but may not give the most efficient method for solving simultaneous congruences.

**Example 3.13** Solve the following system of congruences

\[ x \equiv 1 \mod 3 \]
\[ x \equiv 5 \mod 8 \]
\[ x \equiv 11 \mod 17 \]

We write down the numbers \( m_{ij} \)

\[
\begin{pmatrix}
m_{12} & m_{13} \\
m_{21} & m_{23} \\
m_{31} & m_{32}
\end{pmatrix}
= 
\begin{pmatrix}
2 & 2 \\
3 & 1 \\
6 & 15
\end{pmatrix}
\]

Therefore the solution is

\[
x \equiv c_1 m_{12} n_2 m_{13} n_3 + c_2 m_{21} n_1 m_{23} n_3 + c_3 m_{31} n_1 m_{32} n_2 \\
\equiv 2 \cdot 8 \cdot 2 \cdot 17 + 5 \cdot 3 \cdot 3 \cdot 17 + 11 \cdot 6 \cdot 3 \cdot 15 \cdot 8 \\
\equiv 181
\]

modulo \( 3 \times 8 \times 17 \).

**Alternative (more efficient) solution method.** From the first congruence, we have \( x = 1 + 3t \) for some \( t \in \mathbb{Z} \). Substituting this into the second congruence gives

\[
3t \equiv 4 \mod 8
\]

Since \( 3 \times 3 \equiv 1 \mod 8 \), we can multiply both sides of the above by 3 to get

\[
t \equiv 4 \mod 8.
\]

Hence \( t = 4 + 8r \) for some \( r \in \mathbb{Z} \), so \( x = 3(4 + 8r) + 1 = 13 + 24r \). Substituting this into the third congruence

\[
13 + 24r \equiv 11 \mod 17
\]

Note that \( 24 \equiv 7 \mod 17 \), and \( 7 \times 5 \equiv 35 \equiv 1 \mod 15 \), we have

\[
r \equiv 5 \times (11 - 13) \\
\equiv 7 \mod 17
\]

Therefore \( r = 7 + 17z \) for some \( z \in \mathbb{Z} \). Hence \( x = 13 + 24(7 + 17z) = 181 + 408z \). So the solution is

\[
x \equiv 181 \mod 408.
\]

**Example 3.14** Solve the following polynomial congruence \( x^2 + 2x + 1 \equiv 25 \mod 45 \).

The Chinese remainder theorem can be applied in this situation.
**Corollary to CRT:** Let $f$ be a polynomial with integer coefficients, then

$$f(x) \equiv a \mod n$$

if and only if

$$f(x) \equiv a \mod p^{a_1}$$

$$\vdots$$

$$f(x) \equiv a \mod p^{a_r}$$

**Solution:** The above result means we can decompose the congruence $x^2 + 2x + 1 \equiv 25 \mod 45$ by factorising $45 = 3^2 \times 5$ to give the system

$$(x + 1)^2 \equiv 7 \mod 9$$

$$(x + 1)^2 \equiv 0 \mod 5$$

which has the same solutions mod 45. This system can be solved by brute force. Since $1^2 \equiv 1, 2^2 \equiv 4, 4^2 \equiv 7, 5^2 \equiv 7, 7^2 \equiv 5, 8^2 \equiv 1 \mod 9$. We have

$$x + 1 = 4 \text{ or } 5 \mod 9$$

and

$$x + 1 \equiv 0 \mod 5.$$ 

This gives the systems

$$x \equiv 3 \mod 9 \quad \text{and} \quad x \equiv 4 \mod 9$$

$$x \equiv 4 \mod 5 \quad \quad x \equiv 4 \mod 5$$

We can solve these systems as we did previously.

Let $x = 4 + 5k$ for some $k \in \mathbb{Z}$, then $4 + 5k \equiv 3 \mod 9$ implies $k \equiv 2 \times (3 - 4) \mod 9$. Hence $x \equiv 4 + 5 \times 7 \equiv 39 \mod 45$.

Let $x = 4 + 5k$ for some $k \in \mathbb{Z}$, then $4 + 5k \equiv 4 \mod 9$ implies $k \equiv 0 \mod 9$. Hence $x \equiv 4 \mod 45$.

By the Corollary to the Chinese remainder theorem, $x \equiv 4, 39 \mod 45$ are the solutions to $x^2 + 2x + 1 \equiv 25 \mod 45$.

**Example 3.15** Does the congruence $x^2 + 2x + 1 \equiv 23 \mod 180$ have a solution?

Using the same technique as above, the solutions of the above congruence are precisely the solutions of the system

$$(x + 1)^2 \equiv 3 \mod 4$$
\[(x + 1)^2 \equiv 5 \mod 9 \]
\[(x + 1)^2 \equiv 3 \mod 5 \]

The first congruence has no solutions (why?), therefore the original congruence also has no solutions.

**Note 3.16** We will study quadratic congruences later in the course.

Finally we state the general form of the Chinese remainder theorem (where \(n_1, \ldots, n_r\) are not necessarily pairwise coprime).

**Theorem 3.17** Let \(m_1, \ldots, m_r \in \mathbb{N}\) and \(a_1, \ldots, a_r \in \mathbb{Z}\). The system of congruences

\[
\begin{align*}
  x & \equiv a_1 \mod m_1 \\
  & \vdots \\
  x & \equiv a_r \mod m_r
\end{align*}
\]

has a solution if and only if \(a_i \equiv a_j \mod \gcd(m_i, m_j)\) for all \(i \neq j\).

### 4 Units modulo \(n\)

#### 4.1 Units modulo a prime \(p\)

The following is another way (how did we do it before?) to find the inverse of an element modulo \(p\).

**Theorem 4.1** (Fermat’s little theorem) Let \(p\) be a prime and \(0 < a < p\). Then \(a^{p-1} \equiv 1 \mod p\).

**Proof:** We do this by induction. Suppose \(a^p \equiv a \mod p\). Then

\[
\begin{align*}
  (a + 1)^p & \equiv a^p + a^{p-1} \binom{p}{1} + \cdots + a \binom{p}{p-1} + 1 \\
  & \equiv a^p + 1 \\
  & \equiv a + 1
\end{align*}
\]

Since \(1^p \equiv 1 \mod p\), the result is true for all integers \(a \in \mathbb{Z}\). \(\square\)

We say that the **order** of \(0 < a < p\) is the minimal integer \(m\) such that \(a^m \equiv 1 \mod p\).
Theorem 4.2 Let \( p \) be a prime. Then there exists \( 0 < a < p \) such that \( \{a, a^2, \ldots, a^{p-1}\} = \{1, \ldots, p-1\} \). In other words, there is an element \( 0 < a < p \) such that the powers of a cycle through the nonzero integers modulo \( p \).

Proof: By Fermat’s little theorem, the polynomial \( X^{p-1} - 1 \) has \( p-1 \) distinct roots modulo \( p \). Let \( d \) be any factor of \( p-1 \). Then \( X^d - 1 \) divides \( X^{p-1} - 1 \), and it has exactly \( d \) distinct roots modulo \( p \). Now factor \( p-1 = q_1^{e_1} \cdots q_r^{e_r} \). Then letting \( d = q_i^{e_i} \) and \( d = q_i^{e_i-1} \) shows that the number of elements with order \( q_i^{e_i} \) is exactly \( q_i^{e_i} - q_i^{e_i-1} \). In particular, there exist elements with order \( q_i^{e_i} \) for each \( i = 1, \ldots, r \).

Choose an element \( a_i \) with order \( q_i^{e_i} \). By the following lemma, \( a_1 \cdots a_r \) has order \( p - 1 \). \( \square \)

Lemma 4.3 Let \( 0 < a, b < p \) with orders \( r, s \) respectively. If \( \gcd(r, s) = 1 \), then the order of \( ab \) is equal to \( rs \).

Proof: Homework. \( \square \)

Definition 4.4 An element \( a \) satisfying the conclusions of the above theorem is called primitive root modulo \( p \).

Corollary 4.5 Let \( p \) be a prime. If \( a \) is a primitive root mod \( p \), then \( a^j \equiv 1 \) implies \( p - 1 \) divides \( j \).

We see that primitive roots mod \( p \) always exist. In this case, we say that the units mod \( p \) are cyclic. This is not always true, as we discuss in §4.3.

There is no algorithm to find primitive roots modulo \( p \).

The proof of Theorem 4.2 actually tells us how many primitive roots there are modulo \( p \). This will lead us to the definition of Euler’s totient function \( \varphi \).

Corollary 4.6 Let \( a \) be a prime and \( p - 1 = q_1^{e_1} \cdots q_r^{e_r} \) be a prime factorisation of \( p - 1 \). Then the number of primitive roots modulo \( p \) is equal to

\[
\varphi(p - 1) = \prod_{i=1}^{r} (q_i^{e_i} - q_i^{e_i-1})
\]
Proof: From the proof, there are exactly $q_i^{e_i} - q_i^{e_i-1}$ ways of choosing an element with order $q_i^{e_i}$. Thus $\varphi(p - 1)$ ways of choosing an element with order $p - 1$.

We will discuss the totient function further in the next subsection.

An amusing corollary of the cyclicity of units modulo $p$ (Theorem 4.2) is Wilson’s theorem.

**Theorem 4.7 (Wilson’s theorem)** Let $p$ be a prime. Then $(p - 1)! \equiv -1 \mod p$.

**Proof:** By Theorem 4.2, the elements $0 < a < p$ modulo $p$ can be written as $a, a^2, \ldots, a^{p-1} = 1$ for some primitive root $a$. We see that for $0 < i < p - 1$ we have $a^i \cdot a^{p-1-i} = a^{p-1} = 1$. Moreover $a^i = a^{p-1-i}$ if and only if $i = \frac{p-1}{2}$. This means each element in $\{1, \ldots, p-1\}$ is paired up with a distinct inverse, except for $a^{\frac{p-1}{2}}$ and $a^{p-1} = 1$. In particular, there are exactly two elements such that their square is 1 namely $a^{p-1} = 1$ and $a^i$. In other words:

$$(p - 1)! = a^{\frac{p-1}{2}} a^{p-1} \prod_{i=1}^{\frac{p-1}{2}} a^i a^{p-1-i} \equiv a^{\frac{p-1}{2}}$$

Now $(a^{\frac{p-1}{2}})^2 \equiv 1$, so $a^{\frac{p-1}{2}} \equiv \pm 1$. Since $a$ is a primitive root, we must have $a^{\frac{p-1}{2}} \equiv -1$. This proves the theorem. \(\square\)

### 4.2 Euler’s totient function

In the previous section, we saw that the number of units modulo $p$ is equal to $\varphi(p - 1) = \prod_{i=1}^{r} (q_i^{e_i} - q_i^{e_i-1})$ where $q_i^{e_i} \cdots q_r^{e_r}$ is the prime factorisation of $p - 1$.

This is equal to the value of Euler’s totient function at $n = p - 1$, which counts the number of integers less than $n$ coprime to $n$.

**Definition 4.8 (Totient function)** Let $n \in \mathbb{N}$, then

$$\varphi(n) = \sum_{\gcd(a,n)=1}^{1} \frac{1}{0 < a < n}$$

This is a fundamental function in number theory. We have already seen these two facts.
1. If \( p \) is prime, the number of primitive units modulo \( p \) is equal to \( \varphi(p - 1) \).

2. Let \( n \in \mathbb{N} \), then the number of elements in \( \{0, \ldots, n - 1\} \) which has an inverse modulo \( n \) is equal to \( \varphi(n) \). This is because, by Corollary \( \text{3.10} \) that \( a \in \{0, \ldots, n - 1\} \) has an inverse modulo \( n \) if and only if \( \gcd(a, n) = 1 \).

One may ask the question: Is (1) true for any integer \( n \)? To wit, is the number of primitive roots modulo \( n \) equal to \( \varphi(n - 1) \)? This will be taken up in the next subsection. For now we will study the basic properties of Euler’s totient function.

The most basic property is that

Proposition 4.9 \( \varphi \) is multiplicative, that is, if \( \gcd(m, n) = 1 \) then \( \varphi(mn) = \varphi(m)\varphi(n) \).

Proof: Let \( S_d = \{a \in \mathbb{Z} \mid 0 < a < d, \gcd(a, d)\} \) be the set of integers between 0 and \( d \) which are coprime to \( d \). By definition \( \varphi(d) = |S_d| \). We show that there is a bijection between \( S_{mn} \) and \( S_m \times S_n \) and comparing cardinalities gives the formula.

Define \( f : S_{mn} \rightarrow S_m \times S_n \) by \( f(a) = (a \mod m, a \mod n) \), and \( g : S_m \times S_n \rightarrow S_{mn} \) by \( g(b, c) = x \) where \( x \) is a solution of the system of congruences

\[
\begin{align*}
  x & \equiv b \mod m \\
  x & \equiv c \mod n.
\end{align*}
\]

Since \( \gcd(m, n) = 1 \), by the Chinese remainder theorem (c.f. Theorem 3.12) the solution \( x \) is unique mod \( mn \). These functions are clearly inverses of each other, so are set bijections. \( \square \)

Proposition 4.10 (Euler’s product formula)

\[
\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)
\]

where the product ranges over the prime factors of \( m \).
Proof: This is simply a different way of writing \( \varphi \). Recall that \( \varphi(m) = \prod_{i=1}^{r} (q_i^{e_i} - q_i^{e_i - 1}) \) where \( q_i^{e_i} \cdot \ldots \cdot q_r^{e_r} \) is the prime factorisation of \( m \). Taking out the \( q_i^{e_i} \) factors give the formula.

Proposition 4.11

\[ \sum_{d \mid n} \varphi(d) = n \]

Proof: We do this by induction. The above formula is trivial \( n = 1 \). Assume that the above formula holds for all integers \( < n \). Let \( \alpha \) be the largest power of \( p \) dividing \( n \). Then

\[
\sum_{d \mid n} \varphi(d) = \sum_{i=0}^{\alpha} \sum_{d \mid n/p^i} \varphi(p^i d)
\]

\[
= \sum_{i=0}^{\alpha} \varphi(p^i) \sum_{d \mid n/p^i} \varphi(d)
\]

\[
= \frac{n}{p^\alpha} \sum_{i=0}^{\alpha} \varphi(p^i)
\]

\[
= \frac{n}{p^\alpha} \sum_{i=0}^{\alpha} (p^i - p^{i-1})
\]

\[
= \frac{n}{p^\alpha} \left( (p^\alpha - p^{\alpha-1}) + (p^{\alpha-1} - p^{\alpha-2}) + \cdots + (p^2 - p) + (p - 1) + 1 \right)
\]

\[= n. \]

4.3 Existence of primitive roots

Primitive roots do not always exist mod \( n \).

Example 4.12 Let \( n = 8 \). The units mod 8 are 1, 3, 5, 7. We have \( 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \), so there is no primitive root mod 8.

Theorem 4.13 (Euler) Let \( a, m \in \mathbb{N} \) such that \( \gcd(a, m) = 1 \). Then \( a^{\varphi(m)} \equiv 1 \) mod \( m \).
Proof: Let \( S = \{ x \in \mathbb{N} \mid \gcd(x, m) = 1, 0 < a < m \} \), then \( |S| = \varphi(m) \).

Let \( a \in S \), then \( aS = S \). Hence
\[
\prod_{s \in S} s \equiv \prod_{s \in S} as \equiv a^{\varphi(m)} \prod_{s \in S} s \mod m.
\]

By Corollary 3.10, we can cancel \( \prod_{s \in S} s \) from both sides, leaving \( a^{\varphi(m)} \equiv 1 \mod m \). □

Lemma 4.14 Let \( p \) be a prime and \( a \) be a primitive root mod \( p^\alpha \). Suppose that \( a^k \equiv 1 \mod p^\alpha \), then \( \varphi(p^\alpha) \mid k \).

Proof: Write \( k = i\varphi(p^\alpha) + j \) for some \( 0 \leq j < \varphi(p^\alpha) \). Then \( a^k \equiv a^j \mod p^\alpha \), so \( j = 0 \). □

Proposition 4.15 Let \( p \) be a prime. Then there exists a primitive root mod \( p^2 \).

Proof: Let \( g \) be a primitive root mod \( p \). Then \( g^{p-1} \equiv 1 + tp \mod p^2 \) for some \( 0 \leq t < p \). Let \( h = g + (t - 1)p \), then mod \( p^2 \), we have
\[
h^{p-1} \equiv (g + (t - 1)p)^{p-1} \\
\equiv g^{p-1} + (p - 1)(t - 1)p \\
\equiv 1 + tp - (t - 1)p \\
\equiv 1 + p.
\]

It suffices to prove the following claim: the smallest positive \( j \) such that \( h^j = 1 \) is \( \varphi(p^2) \).

Suppose that \( h^N \equiv 1 \mod p^2 \) for some \( 0 \leq N < \varphi(p^2) \). Since \( h \) is a primitive root mod \( p \), by Lemma 4.14 we must have \( p - 1 \mid N \). Write \( N = j(p - 1) \). Then \( h^N \equiv (1 + p)^j \equiv 1 + jp \mod p^2 \). Hence \( j = 0 \) so \( h^N \equiv 1 \mod p^2 \) for any \( N = 1, \ldots, \varphi(p^2) - 1 \). This shows \( h \) is a primitive root mod \( p^2 \). □

Proposition 4.16 Let \( p \) be an odd prime and suppose that there exists a primitive root mod \( p^2 \). Then there exists a primitive root mod \( p^\alpha \) for all \( \alpha \geq 2 \).

Proof: We show that, under the hypotheses above, if \( g \) is a primitive root mod \( p^\alpha \), then it is a primitive root mod \( p^{\alpha+1} \). Note that \( g \) is a primitive root mod \( p^{\alpha-1} \) (homework), so we can write \( g^{\varphi(p^{\alpha-1})} \equiv 1 + tp^{\alpha-1} \mod p^{\alpha+1} \) with \( 0 \leq t < p^2 \). Note that \( p \) does not divide \( t \), since if \( t = rp \) for some
If \( r \in \mathbb{Z} \), then \( g^{\varphi(p^\alpha - 1)} \equiv 1 \mod p^\alpha \) contradicting \( g \) is a primitive root mod \( p^\alpha \). Therefore, mod \( p^{\alpha + 1} \), we have

\[
g^{\varphi(p^\alpha)} \equiv (1 + tp^{\alpha - 1})^p \\
\equiv 1 + tp^\alpha + \sum_{k=2}^{p} \binom{p}{k} (tp^{\alpha - 1})^k
\]

For \( \alpha \geq 2 \) and \( k \geq 3 \) we have \( k\alpha - k \geq \alpha + 1 \) so \( \binom{p}{k} (tp^{\alpha - 1})^k \equiv 0 \mod p^{\alpha + 1} \). For \( \alpha \geq 2 \) and \( k = 2 \), we have \( \binom{p}{2} (tp^{\alpha - 1})^2 = \frac{p-1}{2} t p^{2\alpha - 1} \equiv 0 \mod p^{\alpha + 1} \) since \( \frac{p-1}{2} \in \mathbb{Z} \) and \( 2\alpha - 1 \geq \alpha + 1 \). This shows that

\[
g^{\varphi(p^\alpha)} \equiv 1 + tp^\alpha \mod p^{\alpha + 1}
\]

which is not congruent to 1 mod \( p^{\alpha + 1} \) since \( p \) does not divide \( t \). We show that \( g^j /\equiv 1 \mod p^{\alpha + 1} \) for all \( j = 1, \ldots, \varphi(p^{\alpha + 1}) - 1 \). Suppose \( g^N \equiv 1 \mod p^{\alpha + 1} \) for some \( 0 \leq N < \varphi(p^{\alpha + 1}) \). Since \( g \) is a primitive root mod \( p^\alpha \), by Lemma 4.14 we must have \( \varphi(p^\alpha) \mid j \). Write \( N = j\varphi(p^\alpha) \) for some \( 0 \leq j < p \) so

\[
g^N \equiv 1 + jtp^\alpha \mod p^{\alpha + 1}
\]

If \( j \neq 0 \), then \( \gcd(jt, p) = 1 \), which contradicts \( g^N \equiv 1 \mod p^{\alpha + 1} \). Hence \( j = 0 \), so \( N = 0 \). This shows that \( g \) is a primitive root mod \( p^{\alpha + 1} \). □

The above proposition is false if \( p = 2 \). In fact, we have the following.

**Proposition 4.17** Let \( n = 2^\alpha \) for \( \alpha \geq 3 \). Then there is no primitive root mod \( n \).

**Proof:** Example 4.12 shows there there is no primitive root mod 8. Let \( \alpha > 3 \) and suppose \( g \) is a primitive root mod \( 2^\alpha \).

If \( g \) is not a primitive root mod \( 2^{\alpha - 1} \), then \( g^i \equiv 1 + 2^{\alpha - 1} \mod 2^\alpha \) for some \( 0 < i < \varphi(2^{\alpha - 1}) \). Squaring this gives \( g^{2i} \equiv (1 + 2^{\alpha - 1})^2 \equiv 1 \mod 2^\alpha \). Since \( 0 < 2i < 2\varphi(2^{\alpha - 1}) = \varphi(2^\alpha) \). This contradicts \( g \) is a primitive root mod \( 2^\alpha \).

Hence \( g \) must be a primitive root mod \( 2^{\alpha - 1} \). Applying this argument \( \alpha - 3 \) times give a contradiction. This proves the proposition. □

**Proposition 4.18** Let \( p \) be an odd prime, then there is a primitive root mod \( 2p^\alpha \).
Proof: Let $\bar{g} \in \mathbb{Z}$ with $0 < \bar{g} < p^a$ be a primitive root mod $p^a$. If $\bar{g}$ is odd, let $g = \bar{g}$, if $\bar{g}$ is even, let $g = \bar{g} + p^a$. Then $g$ is a primitive root mod $2p^a$. If $\bar{g}^i \equiv 1 \mod 2p^a$ for some $0 \leq i < \varphi(2p^a)$, then $\bar{g}^{2i} \equiv 1 \mod p^a$ (why?). This is a contradiction (why?). □

Proposition 4.19 Suppose that $n \not\in \{1, 2, 4, p^a, 2p^a | a \in \mathbb{N}, p \text{ prime}\}$, then there does not exist a primitive root mod $n$.

Proof: We can write $n = ab$ where $a, b > 2$ and $\gcd(a, b) = 1$. Then $\varphi(a)$ and $\varphi(b)$ are both even. Let $e$ be the lcm of $\varphi(a)$ and $\varphi(b)$. Then $e < \varphi(n)$.
For any $0 < g < n$, we have
\[
g^e \equiv 1 \mod a \quad \quad g^e \equiv 1 \mod b
\]
By Theorem 3.12 there is a unique solution mod $n$. Therefore $g^e \equiv 1 \mod n$. This shows that there is no primitive root mod $n$. □

Combining all the results of this subsection, we have proven the following.

Theorem 4.20 Let $n \in \mathbb{N}$, then there exists a primitive root mod $n$ if and only if $n = 1, 2, 4, p^a \text{ a prime or } 2p^a$ where $p$ is prime.

5 Public Key Cryptography

5.1 Application: RSA

The idea of a public-private key cryptosystem is attributed to Diffie and Hellman in 1976.

The encryption scheme we describe below is named for Ron Rivest, Adi Shamir, and Leonard Adleman at MIT (1977).

Let $0 < k < \varphi(m)$ with $\gcd(k, \varphi(m)) = 1$. Then by Corollary 3.10 there is an inverse $k'$ of $k$ mod $\varphi(m)$. Then for any $a$ with $\gcd(a, m) = 1$, we have
\[a^{kk'} \equiv a \mod m.
\]
A consequence of this fundamental congruence is that the power map $r \mapsto r^k$ permutes the units mod $m$. The power map $r \mapsto r^{k'}$ is the inverse permutation mod $m$.

Let $m = pq$ where $p, q$ are large primes. Then
Public key: $m, k$ (this is made available to everybody)
Private key: $p, q$ (this is kept secret)
To send message to someone with the private key, use the public key to encode the message $r$ by calculating $c \equiv r^k \mod m$.
To decrypt the message, do $c^{k'} \equiv r^{kk'} \equiv r \mod m$.
Why does this work? It’s very hard to find $k'$ without knowledge of $p$ and $q$, since we need to know $\varphi(m)$, and computing $\varphi(m)$ is as hard as factoring $m$.
We can also use this for electronic signatures: the holder of the private key uses his private key to encrypt a signature $r$ by $c \equiv r^{k'} \mod m$. Everybody else can verify the signature by doing $c^{k} \equiv r^{kk} \equiv r \mod m$.

6 Quadratic residues and quadratic reciprocity

6.1 Euler’s criterion for quadratic residues mod $p$
Let $p$ be an odd prime. Consider the following quadratic congruence mod $p$

$$ax^2 + bx + c \equiv 0.$$ 

We assume that $\gcd(a, p) = 1$, since otherwise we just get a linear congruence. By Corollary 3.10 we can multiply by the inverse of $a$ to put the congruence in the form

$$x^2 + bx + c \equiv 0$$

Furthermore, since $p$ is odd, there exists $b'$ such that $2b' = b$. This allows us to complete the square

$$(x + b')^2 \equiv (b')^2 - c$$

This reduces the general quadratic congruence to one of the form

$$x^2 \equiv a \mod p.$$ 

Unlike quadratic equations over complex numbers, this congruence does not always have a solution. For example $x^2 \equiv 2 \mod 3$ has no solutions. If $\text{[5]}$ has a solution, we say that $a$ is a quadratic residue mod $p$. The following theorem of Euler gives necessary and sufficient conditions for $a$ to be a quadratic residue mod $p$. 

25
Theorem 6.1 (Euler) Let p be an odd prime and assume that \( \gcd(a, p) = 1 \). Then a is a quadratic residue mod p if and only if
\[
a^{(p-1)/2} \equiv 1 \pmod{p}.
\] (5)

If (5) then there are exactly 2 solutions (mod p) to the congruence \( x^2 \equiv a \pmod{p} \).

Proof: Suppose a is a quadratic residue mod p. Then (5) follows from Fermat’s little theorem (c.f. Theorem 4.1). Indeed, suppose \( x^2 \equiv a \) for some \( x \). Then \( a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \).

Conversely, suppose (5) holds. Let \( g \) be a primitive root mod p, then by Theorem 4.2 we have \( g' \equiv a \). Suppose that \( r \) is odd, so we can write \( r = 2k + 1 \). Then by Theorem 4.1 we have \( a^{(p-2)/2} \equiv g^{(2k+1)(p-1)/2} \equiv g^{k(p-1)}g^{(p-1)/2} \equiv g^{(p-1)/2} \equiv 1 \) which contradicts Corollary 4.5. Hence \( r \) is even. But this means a is a quadratic residue mod p so we are done. \( \square \)

6.2 \( N \)-th power residues

There is a higher order version of this which we can use to prove a theorem about Fermat primes. We say that \( a \) is an \( n \)-th power residue mod \( p \) if \( x^n \equiv a \pmod{p} \) has a solution.

Theorem 6.2 Let \( p \) be an odd prime, then a is an \( n \)-th power residue mod \( p \) if and only if
\[
a^{(p-1)/d} \equiv 1 \pmod{p}
\] (6)

where \( d = \gcd(n, p - 1) \). Moreover, if (6) holds, then the congruence \( x^n \equiv a \pmod{p} \) has \( d \) solutions mod \( p \).

Proof: Suppose that \( a \) is an \( n \)-th power residue mod \( p \). Then \( a \equiv x^n \), so \( a^{(p-1)/d} = x^{n(p-1)/d} \equiv 1 \) by Fermat’s little theorem (c.f. Theorem 4.1).

Conversely, suppose (6) holds. Let \( g \) be a primitive root mod \( p \). By Theorem 4.2 we can write \( a \equiv g^s \) and \( x \equiv g^y \) for some \( s, y \in \mathbb{Z} \). We can then rewrite the congruence \( x^n \equiv a \) as
\[
g^{ny} \equiv g^s \pmod{p}.
\]

By Theorem 4.1, the above holds if and only if \( ny \equiv s \pmod{p-1} \). By Theorem 3.9, this has \( d \) solutions if and only if \( d \mid s \). To finish the proof, it suffices to show that (6) implies \( d \mid s \). Suppose not, then write \( s = dk + r \) where \( 0 < r < d \). Then \( 1 \equiv a^{(p-1)/d} \equiv g^{(dk+r)(p-1)/d} \equiv g^{k(p-1)}g^{r(p-1)/d} \). Since \( r(p-1)/d < p-1 \) this contradicts Corollary 4.5. Hence \( d \mid s \). \( \square \)
6.3 The Legendre symbol

The quadratic reciprocity law relates the question of whether \( p \) is a quadratic residue mod \( q \) to the question of whether \( q \) is a quadratic residue mod \( p \), where \( p, q \) are odd primes. The theorem is rather cumbersome to state in words, so we introduce the Legendre symbol to encode the statement when \( a \) is a quadratic residue mod \( p \).

**Definition 6.3** Let \( p \) be an odd prime. Then

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue mod } p \\
-1 & \text{if } a \text{ is not a quadratic residue mod } p \\
0 & \text{if } p \mid a
\end{cases}
\]

We first prove some basic properties of the Legendre symbol.

**Proposition 6.4**

1. \( \left( \frac{a}{p} \right) = a^{(p-1)/2} \mod p \)

2. \( \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right) \)

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

The first statement is just Euler’s criterion. The proofs of the other two statements are done for homework.

**Proposition 6.5** (Gauss’s Lemma) Let \( p \) be an odd prime and \( a \in \mathbb{Z} \) such that \( \gcd(a, p) = 1 \). Let \( \bar{a} \) denote the integer satisfying \( 0 \leq \bar{a} < p \) and \( \bar{a} \equiv a \mod p \). Consider \( \bar{a}, 2\bar{a}, \ldots, (p-1)a/2 \) and let \( n \) be the number of these \( > p/2 \). Then

\[
\left( \frac{a}{p} \right) = (-1)^n.
\]

**Proof:** We consider the product

\[
\prod_{k=1}^{(p-1)/2} ka = \left( \frac{p-1}{2} \right)!a^{(p-1)/2}.
\]
The set \(a, 2a, \ldots, (p-1)a/2\) consists of distinct elements mod \(p\). Then
\[
\prod_{k=1}^{(p-1)/2} ka \equiv \prod_{0<k<ap/2} ka \prod_{p/2<k<ap} -(p-ka)
\equiv (-1)^n \prod_{0<k<ap/2} ka \prod_{p/2<k<ap} (p-ka)
\equiv (-1)^n \left(\frac{p-1}{2}\right)!
\]
The terms in the two products are all distinct and are between 0 and \(p/2\), hence is just \(\left(\frac{p-1}{2}\right)!\). Combining this with the first equation and cancelling \(\left(\frac{p-1}{2}\right)!\) from both sides (why can we do this?) gives \(a^{(p-1)/2} \equiv (-1)^n\). The lemma follows from Euler’s criterion Theorem 6.1. \(\square\)

**Proposition 6.6 (Eisenstein’s Lemma)** Let \(p\) be an odd prime and \(\gcd(a,2p) = 1\). Then
\[
\left(\frac{a}{p}\right) = (-1)^t
\]
where \(t = \lfloor a/p \rfloor + \lfloor 2a/p \rfloor + \cdots + \lfloor \left(\frac{p-1}{2}\right) a/p \rfloor = \sum_{k=1}^{(p-1)/2} \lfloor ka/p \rfloor\).

**Proof:** We can work modulo 2 in the proof, since \((-1)^t = (-1)^t'\) if \(t \equiv t' \mod 2\). We consider the difference
\[
\sum_{k=1}^{(p-1)/2} ka - \sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{(p-1)/2} p\lfloor ka/p \rfloor + \sum_{k=1}^{(p-1)/2} ka - \sum_{k=1}^{(p-1)/2} k.
\]
If \(0 < ka < p/2\), then \(ka\) will cancel with a term in the last sum. If \(p/2 < ka < p\), then \(p - ka\) appears in the last sum. Hence we can rewrite the above as
\[
(a-1) \left(\sum_{k=1}^{(p-1)/2} k\right) = \sum_{k=1}^{(p-1)/2} p\lfloor ka/p \rfloor + \sum_{p/2<ka<p} p - 2(p-ka). \quad (7)
\]
Since \(a\) is odd, we can take the above mod 2, to get
\[
n \equiv \sum_{k=1}^{(p-1)/2} \lfloor ka/p \rfloor \mod 2.
\]
\(\square\)
Lemma 6.7 Let $p$ be an odd prime, then

$$\left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}$$

Proof: Homework.

6.4 Application

Theorem 6.8 (Euler) Every factor of $F_n := 2^{2^n} + 1$ is of the form $k2^{n+1} + 1$ for some $k \in \mathbb{Z}$.

Proof: It suffices to prove this for prime factors $p$ of $F_n$ (why?). Let $o$ denote the order of 2 mod $p$. We show that $o = 2^{n+1}$. Since $2^{2^n} + 1 \equiv 0$ mod $p$, we have $2^{2^n} \equiv -1$ mod $p$ so $2^{2^n+1} \equiv 1$ mod $p$. Hence $o = 2^r$ for some $r \in \mathbb{N}$. Suppose $r < n+1$. Then $(2^2)^{2^{n-r}} \equiv 2^{2^n} \equiv 1$ which is a contradiction. Therefore $r = n+1$, i.e. $o = 2^{n+1}$. Now $2^{p-1} \equiv 1$ mod $p$, so $2^{n+1} \mid p-1$. This proves the theorem.

Theorem 6.9 (Lucas) Assume $n \geq 2$. Then every factor of $F_n$ is of the form $k2^{n+2} + 1$ for some $k \in \mathbb{Z}$.

Proof: Again it suffices to prove this for prime factors $p$ of $F_n$. Let $p$ be a prime factor of $F_n$. Since $n \geq 2$, by Theorem 6.8, we see that $p = 8t + 1$ for some $t \in \mathbb{Z}$. By Lemma 6.7, we have that 2 quadratic residue mod $p$. By Theorem 6.1 we have

$$2^{p-1} \equiv 1 \mod p$$

Therefore $o = 2^{n+1}$ (c.f. proof of Theorem 6.8) divides $\frac{p-1}{2}$. This proves the theorem.

6.5 Quadratic reciprocity

Theorem 6.10 Let $p \neq q$ be odd primes. Then

$$\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}.$$
Note 6.11 This is a very compact way of saying the following. Firstly, since $p$ is an odd prime, we have

$$\frac{p - 1}{2} \begin{cases} \text{even if} & p \equiv 1 \mod 4 \\ \text{odd if} & p \equiv 3 \mod 4 \end{cases}.$$  

In other words, in all cases except for $p \equiv q \equiv 3 \mod 4$, \((\frac{p}{q}) = (\frac{q}{p})\), that is, $p$ is a quadratic residue mod $p$ if and only if $q$ is a quadratic residue mod $q$.

In the case where both $p \equiv q \equiv 3 \mod 4$, \((\frac{p}{q}) = -(\frac{q}{p})\), that is, $p$ is a quadratic residue mod $p$ if and only if $q$ is not a quadratic residue mod $p$.

Example 6.12 Does the congruence $x^2 \equiv 5 \mod 103$ have solution(s)? Since $5 \equiv 1 \mod 4$, by quadratic reciprocity, this congruence has solution(s) if and only if $x^2 \equiv 103 \equiv 3 \mod 5$ have solution(s). The Legendre symbol \((\frac{3}{5})\) is easy to compute, it’s just $3^2 \equiv -1 \mod 5$. Hence neither congruence have solutions.

If we didn’t use quadratic reciprocity, we only have Euler’s criterion, meaning we have to compute $5^{51} \mod 103$.

Proof: (of quadratic reciprocity) We show that \(\left(\frac{p-1}{2}\right) \left(\frac{q-1}{2}\right) = \sum_{k=1}^{(p-1)/2} \left[ kp / p \right] + \sum_{k=1}^{(q-1)/2} \left[ kp / q \right]\). Then the theorem will follow from Proposition 6.6.

Consider the set $S = \{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 < x < (p-1)/2, 0 < y < (q-1)/2 \}$. Then $|S| = \left(\frac{p-1}{2}\right) \left(\frac{q-1}{2}\right)$. We write $S$ as union $S = S_+ \cup S_-$ where $S_+ = \{ (x, y) \in S \mid qx < py \}$ and $S_- = \{ (x, y) \in S \mid qx > py \}$. This is a disjoint union, since $qx = py$ is impossible. Hence $|S| = |S_+| + |S_-|$.

Now $|S_+| = \sum_{y=1}^{(q-1)/2} \left[ py / q \right]$ and $|S_-| = \sum_{x=1}^{(p-1)/2} \left[ qx / p \right]$, so we are done. \[ \square \]

The theorem of quadratic reciprocity, combined with Proposition 6.4 give us effective ways to compute the Legendre symbol \(\left(\frac{a}{p}\right)\). However the quadratic reciprocity law as stated only applies to the case where both numbers in the Legendre symbol are prime. We can get around this by factorisation, but this is unnecessary.

Definition 6.13 For $a, b \in \mathbb{Z}$, define the Jacobi symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$$

where $p_1, \ldots, p_r$ are prime and $p_1 \cdots p_r = b$.  

30
While the Jacobi symbol helps us compute the Legendre symbol, it does not have the same meaning if \(a, b\) are not prime. If \(a\) is a square mod \(b\), then \((\frac{a}{b}) = 1\), but the converse is false!

**Example 6.14** For example \((\frac{2}{15}) = 1\) but the congruence \(x^2 \equiv 2 \mod 15\) does not have solutions! That is 2 is not a quadratic residue mod 15. In order for this congruence to have a solution, it is necessary and sufficient that

\[
\begin{align*}
x^2 &\equiv 2 \mod 3 \\
x^2 &\equiv 2 \mod 5
\end{align*}
\]

both have solutions. That is 2 is a quadratic residue mod 3 and 5. In other words, if

\[
\left(\frac{2}{3}\right) = 1 \quad \left(\frac{2}{5}\right) = 1.
\]

**Proposition 6.15** Let \(p\) be an odd prime. If \(a\) is a quadratic residue mod \(p^\alpha\) for some \(\alpha > 0\), then \(a\) is a quadratic residue mod \(p^{\alpha+1}\).

**Proof:** Homework. \(\square\)

**Proposition 6.16** Let \(n = p_1^{e_1} \cdots p_r^{e_r}\) be the prime factorisation of \(n\) and let \(a \in \mathbb{Z}\) with \(\gcd(a, n) = 1\). Assume that \(n\) is odd. Then \(a\) is a quadratic residue mod \(n\) iff

\[
\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \cdots = \left(\frac{a}{p_r}\right) = 1.
\]

In particular, there are exactly \(\varphi(n)/2^r\) quadratic residues mod \(n\).

**Theorem 6.17** Let \(a, a', b, b'\) be positive integers. Assume that \(b, b'\) are odd.

1. (congruence) if \(a \equiv a' \mod b\) then \((\frac{a}{b}) = (\frac{a'}{b})\)
2. (factorisation) \((\frac{a a'}{b}) = (\frac{a}{b}) (\frac{a'}{b})\) and \((\frac{a}{b b'}) = (\frac{a}{b}) (\frac{a}{b'})\)
3. (QR) \((\frac{-1}{b}) = (-1)^{(b-1)/2}, (\frac{2}{b}) = (-1)^{(b^2-1)/8}\) and if \(a\) is odd \((\frac{a}{b}) (\frac{b}{a}) = (-1)^{(a-1)(b-1)/4}\).
Proof: Exercise, these all follow from the theorems above. □

Example 6.18 Compute \(\left(\frac{17}{1123}\right)\).

\[
\left(\frac{17}{1123}\right) = (-1)\frac{1123 - 16}{2} \left(\frac{1123}{17}\right) = \left(\frac{1}{17}\right) = 1.
\]

Example 6.19 Compute \(\left(\frac{1123}{2311}\right)\).

Since \(1123 \equiv 2311 \equiv 3 \mod 4\), we have

\[
\left(\frac{1123}{2311}\right) = -\left(\frac{2311}{1123}\right) = -\left(\frac{65}{1123}\right)
\]

Since \(65 \equiv 1 \mod 4\), we have

\[
\left(\frac{65}{1123}\right) = \left(\frac{1123}{65}\right) = \left(\frac{18}{65}\right) = \left(\frac{2}{65}\right) \left(\frac{3^2}{65}\right) = \left(\frac{2}{65}\right) = (-1)^{65-1} = 1
\]

Therefore

\[
\left(\frac{1123}{2311}\right) = -1.
\]

The following theorem shows that the smallest quadratic nonresidue mod \(p\) cannot be too large.

Theorem 6.20 Let \(p\) be an odd prime, and \(n\) denote the least quadratic nonresidue mod \(p\). Then \(n > 1 + \sqrt{p}\).

Proof: Let \(m\) be the least positive integer such that \(mn > p\), that is \((m - 1)n < p\). Since \(n \geq 2\) and \(p\) is an odd prime, this inequality is strict. Therefore \(0 < mn - p < n\). Since \(n\) is the least quadratic residue mod \(p\), we have

\[
\left(\frac{mn - p}{p}\right) = 1
\]

hence \(\left(\frac{m}{p}\right) = -1\). Consequently \(m \geq n\) so that

\[(n - 1)^2 < (n - 1)n \leq (m - 1)n < p\]

Thus \(n - 1 < \sqrt{p}\). □