Chapter 1

Integers and Integers mod \( n \)

The Fibonacci sequence is the infinite sequence of integers \( f_i \) for \( i = 1, 2, \ldots \) defined recursively by

\[
f_1 = 1, \quad f_2 = 1, \quad \text{and} \quad f_n = f_{n-2} + f_{n-1} \quad \text{for all integers} \quad n \geq 2. \quad (1.1)
\]

Thus, the initial terms in the Fibonacci sequence are:

\[1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots \]

The integer \( f_n \) is called the \( n \)-th Fibonacci number.

1.1. Prove the closed formula for the Fibonacci sequence:

\[
f_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n \quad (1.2)
\]

(i) Prove formula (1.2) by mathematical induction.

(ii) Prove formula (1.2) by using its generating function: This is the formal power series

\[
g = \sum_{i=1}^{\infty} f_i X^i = X + X^2 + 2X^3 + 3X^4 + 5X^5 + 8X^6 + \ldots .
\]

Use the recursive formula for the \( f_i \) to express \( g \) as a quotient of polynomials. Then find a new series expansion for \( g \) using its partial fractions decomposition.
For another proof of the closed formula (1.2) for the Fibonacci sequence, using linear algebra, see problem 4.44 below. Note that since \(\left|\frac{(1 - \sqrt{5})/2}{\sqrt{5}}\right| < 1\) and \(\frac{1}{\sqrt{5}}\left|\frac{1-\sqrt{5}}{2}\right| < 0.5\) it follows that \(f_n\) is the integer nearest \(\frac{1}{\sqrt{5}}\left((1 + \sqrt{5})/2\right)^n\). For example,

\[ f_{1000} \approx \frac{1}{\sqrt{5}}\left((1 + \sqrt{5})/2\right)^{1000} \approx 4.34666 \times 10^{208}, \]

so \(f_{1000}\) is a 209-digit number.

The **Division Algorithm** for integers says that for any given integers \(a, b\) with \(b \geq 1\) there exist unique integers \(q\) and \(r\) such that

\[ a = qb + r, \quad \text{with} \quad 0 \leq r \leq b - 1. \quad (1.3) \]

Recall that for integers \(a\) and \(b\), we say that \(a\) divides \(b\) (denoted \(a \mid b\)) if there is an integer \(c\) with \(b = ca\). When \(a\) and \(b\) are nonzero, the **greatest common divisor** of \(a\) and \(b\) (denoted \(gcd(a, b)\)) is the largest positive integer dividing both \(a\) and \(b\). The **least common multiple** of \(a\) and \(b\) (denoted \(lcm(a, b)\)) is the smallest positive integer that is a multiple of both \(a\) and \(b\).

Recall the **Euclidean Algorithm** for computing greatest common divisors by repeated application of the Division Algorithm: Take any nonzero integers \(a, b\) with \(b \geq 1\) (and without loss of generality, \(b \leq |a|\)). By the Division Algorithm, we can write successively

\[ a = q_1b + r_1 \quad \text{with} \quad 0 < r_1 \leq b - 1; \]
\[ b = q_2r_1 + r_2 \quad \text{with} \quad 0 < r_2 \leq r_1 - 1; \]
\[ r_1 = q_3r_2 + r_3 \quad \text{with} \quad 0 < r_3 \leq r_2 - 1; \]
\[ \ldots \]
\[ r_{j-2} = q_jr_{j-1} + r_j \quad \text{with} \quad 0 < r_j \leq r_{j-1} - 1; \]
\[ \ldots \]
\[ r_{n-3} = q_{n-1}r_{n-2} + r_{n-1} \quad \text{with} \quad 0 < r_{n-1} \leq r_{n-2} - 1; \]
\[ r_{n-2} = q_nr_{n-1} + 0. \]

The repeated division process terminates when the remainder \(r_n\) hits 0. The process must terminate after finitely many steps because \(b > r_1 > r_2 > \ldots \geq 0\). Then,

\[ gcd(a, b) = r_{n-1}, \quad \text{the last nonzero remainder.} \]
1. Integers and Integers mod $n$

The Euclidean Algorithm shows the existence of $\gcd(a, b)$ and also that $\gcd(a, b)$ is expressible as $sa + tb$ for some integers $s, t$. The number $n$ of times the Division Algorithm is applied is called the number of steps needed in computing $\gcd(a, b)$.

For example, let $f_1, f_2, \ldots$ be the Fibonacci sequence. For an integer $i \geq 2$, the number of steps needed in computing that $\gcd(f_i, f_{i+1}) = 1$
is $i - 1$. (The successive remainders $r_j$ in the long divisions are $f_{i-1}, f_{i-2}, \ldots, f_3, f_2, 0$.)

1.2. Efficiency of the Euclidean Algorithm. Take any nonzero integers $a, b$ with $1 \leq b \leq |a|$, and let $n$ be the number of steps needed in computing $\gcd(a, b)$, as defined above. Let $f_j$ be the $j$-th Fibonacci number. Prove that if $b \leq f_j$, for $j \geq 2$, then $n \leq j - 1$.

The preceding example shows that the bound on $n$ in problem 1.2 is the best possible. This problem shows that determination of greatest common divisors is very efficient from a computational standpoint. Recall that $f_n$ is the integer nearest $\frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^n$. So, if $b$ is a $k$-digit number, then the number of divisions required to compute $\gcd(a, b)$ is at most

$$(k + \log_{10}(\sqrt{5}))/\log_{10}((1 + \sqrt{5})/2) \approx 4.785k + 1.672.$$  

For example, if $b$ is 100-digit number, then $\gcd(a, b)$ can be computed with at most 481 long divisions.

1.3. Let $m, n$ be positive integers with $\gcd(m, n) = 1$. Determine the least integer $k$ such that every integer $\ell \geq k$ is expressible as $\ell = rm + sn$ for some nonnegative integers $r, s$.

For example, if $m = 5$ and $n = 8$, then $k = 28$. Thus, with a supply of 5-cent and 8-cent stamps, one can make exact postage for any amount of 28 cents or more, but not for 27 cents.

Congruence mod $n$. Fix a positive integer $n$. For $a, b \in \mathbb{Z}$ we say that $a$ and $b$ are congruent modulo $n$, denoted

$$a \equiv b \pmod{n},$$

if $n|(b - a)$, i.e., there is some $t \in \mathbb{Z}$ with $b - a = tn$. 


1. Integers and Integers mod \( n \)

Recall the Chinese Remainder Theorem, which says that for all \( m, n \in \mathbb{N} \) with \( \gcd(m, n) = 1 \) and any \( a, b \in \mathbb{Z} \) there is an \( x \in \mathbb{Z} \) such that

\[
x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}.
\]

(1.5)

Moreover, any \( x' \in \mathbb{Z} \) satisfies the same congruence conditions as \( x \) in (1.5) iff \( x' \equiv x \pmod{mn} \). (See Example 2.19 below for a proof of the Chinese Remainder Theorem.)

1.4. Take any \( m, n \in \mathbb{N} \) and let \( d = \gcd(m, n) \). Prove that for any \( a, b \in \mathbb{Z} \) there is an \( x \in \mathbb{Z} \) with

\[
x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n}
\]

iff \( a \equiv b \pmod{d} \). Moreover, when this holds, any \( x' \in \mathbb{Z} \) satisfies the same congruence conditions as \( x \) iff \( x' \equiv x \pmod{lcm(a, b)} \).

1.5. Well-definition of \( \mathbb{Z}_n \) operations.

(i) The formula for \( [a]_n + [b]_n \) in (1.9) is expressed in terms of \( a \) and \( b \). But the choice of the integer \( a \) to describe \([a]_n\) is not unique (see (1.7)). That the sum is well-defined means that if \([a]_n = [a']_n\) and \([b]_n = [b']_n\), then we get the same congruence class for the sum whether the sum is determined...
1. Integers and Integers mod $n$

using $a$ and $b$ or $a'$ and $b'$, i.e., $[a + b]_n = [a' + b']_n$. Prove this.

(ii) Prove that the product operation given in (1.9) is well-defined.

1.6. Fix $n \in \mathbb{N}$ and take any $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$. Prove that for any congruence class $[a]_n$ in $\mathbb{Z}_n$ there is a unique congruence class $[b]_n$ such that $[k]_n \cdot [b]_n = [a]_n$.

1.7.

(i) Prove Wilson’s Theorem: If $p$ is a prime number, then

$$(p - 1)! \equiv -1 \pmod{p}.$$ 

(ii) Prove that if $n \in \mathbb{N}$ is not a prime number, then

$$(n - 1)! \equiv 0 \pmod{n}.$$ 

Euler’s $\varphi$-function (also called Euler’s totient function) is the map $\varphi: \mathbb{N} \to \mathbb{N}$ given by

$$\varphi(n) = |\{k \in \mathbb{N} | 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|. \quad (1.10)$$

Note that for any prime number $p$ and any $r \in \mathbb{N}$, $\varphi(p^r) = p^r - p^{r-1}$. Since $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m, n) = 1$ (see problem 1.9 below), it follows that for distinct prime numbers $p_1, \ldots, p_k$ and positive integers $r_1, \ldots, r_k$ if $n = p_1^{r_1} \cdots p_k^{r_k}$, then

$$\varphi(n) = \prod_{j=1}^{k} (p_j^{r_j} - p_j^{r_j - 1}) = n \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}). \quad (1.11)$$

1.8. Take any $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Prove that for $k \in \mathbb{Z}$, $\gcd(k, mn) = 1$ iff $\gcd(k, m) = 1$ and $\gcd(k, n) = 1$.

1.9. Prove that for $m, n \in \mathbb{N}$,

if $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. \quad (1.12)

(For a proof of this formula using groups, see (2.16) below.)

1.10. Prove that for any $n \in \mathbb{N}$,

$$\sum_{d|n} \varphi(d) = n. \quad (1.13)$$

The sum is taken over all the divisors $d$ of $n$ with $1 \leq d \leq n$. (See Example 2.18 below for a group-theoretic approach to this formula.)
Recall that for integers $n, k$ with $0 \leq k \leq n$ the binomial coefficient $\binom{n}{k}$ is defined by
\[
\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)...(n-k+1)}{k(k-1)(k-2)...1}.
\] (1.14)

An easy calculation from the definition yields Pascal’s Identity:
\[
\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{for all } n, k \in \mathbb{N} \text{ with } 1 \leq k < n. \quad (1.15)
\]

It follows by induction on $n$ that $\binom{n}{k}$ is always an integer. Note that
\[
\text{if } p \text{ is a prime number and } 1 \leq k \leq p-1, \text{ then } p \nmid \binom{p}{k}. \quad (1.16)
\]

For $p \mid \binom{p-1}{k} = (p-k)\binom{p}{k}$. Since $p$ is prime and $p \nmid (p-k)$, $p$ must divide $\binom{p}{k}$.

1.11. Prove Fermat’s Theorem: If $p$ is a prime number, then
\[
a^p \equiv a \pmod{p} \quad \text{for any } a \in \mathbb{Z}.
\]

(Hint: Prove this by induction on $a$ using the binomial expansion.)

See problem 2.4(ii) below for another proof of Fermat’s Theorem.
Suggestions for Further Reading

Here are some suggestions for collateral reading or deeper study in various areas of abstract algebra.

There are a number of very good texts in abstract algebra. These include Artin [1], Dummit & Foote [5], Hungerford [9], Jacobson [10], Knapp [13], and Lang [16]. Dummit & Foote and Hungerford have particularly extensive problem sets. For more on group theory, see Rotman [20] or Hall [7].

In ring and module theory, for commutative rings see Atiyah & MacDonald [2], and for noncommutative rings, see Lam [15].

For linear algebra, see Hoffman & Kunze [8].

Two outstanding texts on Galois theory are the books by Cox [4] and by Tignol [23]. Each has interesting historical commentary on the work of Galois and his predecessors.

For algebraic number theory, there are many good texts, e.g., Marcus [17] and Weiss [24]. Marcus’s book has an outstanding selection of problems.

Two important more advanced areas of algebra not treated here are homological algebra and algebraic geometry. See Rotman [22] for a good introduction to homological algebra. The book by Reid [19] provides a gentle introduction to algebraic geometry; see the references provided there for further reading.
Bibliography

When available, Mathematical Reviews reference numbers are indicated at the end of each bibliographic entry as MR******. See www.ams.org/mathscinet.