Elementary Number Theory

Abhishek (January 29, 2026)

Contents

Chapter 1

Basic number theory

> SUGGESTIONS. For this chapter, state the basic axioms and properties/theorems of $\mathbb{Z}$. Provide proofs. But remember that most of the properties/theorems can be generlized to properties/theorems for rings. It's still a good idea to prove the facts for $\mathbb{Z}$ since $\mathbb{Z}$ is not as abstract as general rings and will prepare you for the general results.

The area of Number theory is huge. We will only cover number theory until we reach prime factorization. The reason being that one of the most important ciphers that is used in the world is based on the difficulty of factorizing two very large prime numbers. SPOLER ALERT IT's RSA.

Since, we now know that the study of number theory is huge, it is also important to know that many different fields of mathematics have advanced because of nubmer theory such as automorphic theory, theory of modular forms, algebraic geometry etc.

The term "elementary" here does not mean that the content is easy rather that is actually the begining of the number thoery. Since, it will take a very long time to begin from nothing and cover everything in number thoery, we will start directly from the study of $\mathbb{Z}$ and it's properties.

We need to think of Z as not just a set in itself, but rather the set including operations $+$, $*$, 0, 1

Chapter 2

Semi-Groups

Let us recall that a group is$(G, *, e)$ where G is a set and $e \in G$ such that it satisfies

1. **Closure:** If $x, y \in G$, then $x * y \in G$. This means that $* : G \times G \to G$ is a binary operation.
2. **Associativity:** If $x, y, z \in G$, then $(x * y) * z = x * (y * z)$.
3. **Inverse:** If $x \in G$, then there is some $y \in G$ such that $x * y = e = y * x$.
4. **Neutral:** If $x \in G$, then $e * x = x = x * e$.

For a semigroup, it is almost a group except you do not need the inverses.

Definition: A semigroup is a tuple $(G, *)$ where G where G is a set and the following are satisfied:

1. **Closure:** If $x, y \in G$, then $x * y \in G$. This means that $* : G \times G \to G$ is a binary operation.
2. **Associativity:** If $x, y, z \in G$, then $(x * y) * z = x * (y * z)$.

Commulative Semigroup $(G, *)$ is a semigroup such that $*$ is commulative, i.e, if $x, y \in G$, then

Definition: A monoid is a tuple $(G, *, e)$ where G is a set and the following are satisfied: Closure, Associativity and Neutral.

And of course a commulative monoid $(G, *, e)$ is a monoid such that $*$ is commulative, i.e, if $x, y \in G$, then $x * y = y * x$

Proposition: Uniqueness of an Identity.

Suppose e, f are identities in G.

$\forall a \; in G \; ae = ea = a$

and $af = fa = a$ Let us take, $a = f$, then, $fe = ef = f$ now, let's assume $a = e$, then $ef = fe = e$

The above statements are only true for $e = f$, thus proving uniqueness.

Chapter 3

Rings and Fields

We can generalize the properties of $\mathbb{Z}$ using rings.

Definition: $(R, +_R, *_R, 0_R, 1_R)$ is a ring if

1. $(R, +_R 0_R)$ is an abelian group
2. $(R, ._R 1_R)$ is an semigroup with Identity
3. Distribution: If $x, y, z \in R$, then, $x *_R (y +_R z) = x *_R y +_R x *_r z$
   $(y +_R z) *_R x = y *_R x +_R z *_r x$

$R, +_R, *_R, 0_R, 1_R)$ is a commulative ring if it is a ring and if $x, y \in R$,

$x *_R y = y *_R x$

Chapter 4

Axioms of $\mathbb{Z}$

$(Z, +, \cdot, 0, 1)$ satisfies:

Properties of $+$

- **Closure**: $\forall x, y \in Z, x + y \in Z$
- **Associativity**: $\forall x, y, z \in Z, (x + y) + z = x + (y + z)$
- **Inverse**: $\forall x \in Z, \exists y$ s.t. $x + y = 0 = y + x$
- **Neutrality**: $\forall x \in Z, 0 + x = x = x + 0$
- **Commutativity**: $\forall x, y \in Z, x + y = y + x$

Properties of $\cdot$

- **Closure**: $\forall x, y \in Z, x \cdot y \in Z$
- **Associativity**: $\forall x, y, z \in Z, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- **Neutrality**: $\forall x \in Z, 1 \cdot x = x = x \cdot 1$
- **Commutativity**: $\forall x, y \in Z, x \cdot y = y \cdot x$

Distributivity $\forall x, y, z \in Z, x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$

Ring Structure
R with ops $+_R, \cdot_R$ and elems $0_R, 1_R$ satisfying above = **commutative ring**.

Without commutativity = **non-commutative ring**.

Example: $M_{n \times n}(R)$ = non-commutative ring.

By convention, "ring" means commutative ring.

Special Properties

- **Integrality**: $\forall x, y \in Z, xy = 0 \Rightarrow x = 0$ or $y = 0$

- **Nontriviality**: $0 \neq 1$

Z is an **integral domain**.

Peano-Dedekind Axioms for $\mathbb{N}$

- **Induction**: If $X \subseteq \mathbb{N}$ with $0 \in X$ and $n \in X \Rightarrow n+1 \in X$, then $X = \mathbb{N}$

Well-Ordering Principle

- **WOP for $\mathbb{N}$**: If $X \subseteq \mathbb{N}$ non-empty, then X has least element
- **WOP for Z**: If $X \subseteq Z$ non-empty and bounded below, then X has least element

Induction Variants

For $\mathbb{N}$

- **Weak Induction**: $0 \in X$ and $n \in X \Rightarrow n+1 \in X$ implies $X = \mathbb{N}$
- **Strong Induction**: $0 \in X$ and $\forall k \leq n, k \in X \Rightarrow n+1 \in X$ implies $X = \mathbb{N}$

For Z

- **Weak Induction**: $P(n_0)$ true and $P(n) \Rightarrow P(n+1)$ implies $P(n)$ true $\forall n \geq n_0$
- **Strong Induction**: $P(n_0)$ true and $[\forall k, n_0 \leq k \leq n, P(k)] \Rightarrow P(n+1)$ implies $P(n)$ true $\forall n \geq n_0$

Order Axioms

- **Trichotomy**: $\forall x \in Z$, exactly one: $-x \in Z^+$, $x = 0$, or $x \in Z^+$
- **Closure of $+$ for Z^+**: $\forall x, y \in Z^+, x + y \in Z^+$
- **Closure of $\cdot$ for Z^+**: $\forall x, y \in Z^+, x \cdot y \in Z^+$

Define $x < y$ if $y - x \in Z^+$

Define $x \leq y$ if $x < y$ or $x = y$

Topology for Z: $\forall x \in Z$, $\nexists y \in Z$ s.t. $x < y < x + 1$

Properties and Theorems

Prop 2.1.1: Uniqueness of additive inverse.
If $x + y = 0 = y + x$ and $x + y' = 0 = y' + x$, then $y = y'$.

Proof: $y = 0 + y = (y' + x) + y = y' + (x + y) = y' + 0 = y'$

Def 2.1.1: $x - y = x + (-y)$

Def 2.1.2: y is multiplicative inverse of x if $xy = 1 = yx$
x is a unit if it has multiplicative inverse.

Prop 2.1.2: Uniqueness of multiplicative inverse.
If $xy = 1 = yx$ and $xy' = 1 = y'x$, then $y = y'$.

Proof: $y = 1y = (y'x)y = y'(xy) = y'1 = y'$

Def 2.1.3: Mult. inverse is x^{-1}. Units: $U(Z) = Z^{\times} = \{-1, 1\}$.

Prop 2.1.3: Cancellation law for addition.
(a) If $x + z = y + z$, then $x = y$.
(b) If $z + x = z + y$, then $x = y$.

Prop 2.1.4: Let $x \in Z$.
(a) $0x = 0 = x0$
(b) $-0 = 0$
(c) $x - 0 = x$

Proof:
(a) $0x = (0 + 0)x = 0x + 0x \Rightarrow 0 + 0x = 0x + 0x \Rightarrow 0 = 0x$
$0 = 0x = x0$ (by commutativity)
(b) $0 + (-0) = 0 = (-0) + 0$ and $0 + 0 = 0 = 0 + 0 \Rightarrow -0 = 0$
(c) $x - 0 = x + (-0) = x + 0 = x$

Prop 2.1.5: Let $x, y, c \in Z$.
(a) $-(-1) = 1$
(b) $-(-x) = x$
(c) $x(-1) = -x = (-1)x$
(d) $(-1)(-1) = 1$
(e) $(-x)(-y) = xy$
(f) $-(x + y) = -x + -y$
(g) $-(x - y) = -x + y$

Proof:
(b) $(-x) + (-(-x)) = 0 = (-(-x)) + (-x)$ and $(-x) + x = 0 = x + (-x) \Rightarrow -(-x) = x$
(a) From (b) with $x = 1$, $-(-1) = 1$
(c) $x + x(-1) = x \cdot 1 + x(-1) = x(1 + (-1)) = x0 = 0 \Rightarrow x(-1) = -x$
(d) $(-1)(-1) = -(-1) = 1$

(e) $(-x)(-y) = (-1)x(-1)y = (-1)(-1)xy = 1xy = xy$
(f) $-(x+y) = (-1)(x+y) = (-1)x + (-1)y = -x + -y$
(g) $-(x-y) = -(x+(-y)) = (-1)(x+(-y)) = (-1)x + (-1)(-y) = -x + (-(-y)) = -x + y$

Prop 2.1.6: Cancellation law for multiplication.
(a) If $xz = yz$ and $z \neq 0$, then $x = y$.
(b) If $zx = zy$ and $z \neq 0$, then $x = y$.

Proof:
$xz = yz \Rightarrow xz + (-yz) = 0 \Rightarrow (x + (-1)y)z = 0 \Rightarrow x + (-1)y = 0$ or $z = 0$
Since $z \neq 0$, $x + (-1)y = 0 \Rightarrow x = -(-1)y = (-1)(-1)y = 1y = y$

Formal Sums and Products: $\sum_{i=1}^{n} x_i = \begin{cases} 0 & \text{if } n = 0 \\ \sum_{i=1}^{n-1} x_i + x_n & \text{if } n > 0 \end{cases}$

$\prod_{i=1}^{n} x_i = \begin{cases} 1 & \text{if } n = 0 \\ \prod_{i=1}^{n-1} x_i \cdot x_n & \text{if } n > 0 \end{cases}$

Chapter 5

Divisibility

Def 2.2.1: Let $a, n \in Z$ with $a \neq 0$. We say a divides b, written $a \mid b$, if $\exists x \in Z$ s.t. $ax = b$.

Prop 2.2.1: Let $a, b, c \in Z$.

- (a) $1 \mid a$.
- (b) $a \mid 0$.
- (c) Reflexivity: $a \mid a$.
- (d) Transitivity: If $a \mid b$ and $b \mid c$, then $a \mid c$.
- (e) Antisymmetry: If $a \mid b$ and $b \mid a$, then $a = \pm b$.
- (f) If $a \mid b$, then $a \mid bc$.
- (g) If $a \mid b$ and $a \mid c$, then $a \mid b + c$.
- (h) Linearity: If $a \mid b, a \mid c$, then $a \mid bx + cy$ for $x, y \in Z$.
- (i) If $a \mid b$, then $|a| \leq |b|$.

Proof:

- (a) $1 \cdot a = a \Rightarrow 1 \mid a$.
- (b) $a \cdot 0 = 0 \Rightarrow a \mid 0$.
- (c) $a \cdot 1 = a \Rightarrow a \mid a$.
- (d) If $a \mid b, b \mid c$, then $\exists x, y \in Z$ s.t. $ax = b, by = c$. Thus $axy = c \Rightarrow a \mid c$.
- (e) If $a \mid b, b \mid a$, then $\exists x, y \in Z$ s.t. $ax = b, by = a$. Thus $bxy = b$, so $b(xy - 1) = 0$. Since $b \neq 0$, $xy - 1 = 0 \Rightarrow xy = 1$. Hence $x = y = 1$ or $x = y = -1$, giving $a = b$ or $a = -b$.
- (f) If $a \mid b$, then $ax = b$. Thus $axc = bc \Rightarrow a \mid bc$.
- (g) If $a \mid b, a \mid c$, then $ax = b, ay = c$. Thus $a(x+y) = ax + ay = b + c \Rightarrow a \mid b + c$.
- (h) If $a \mid b, a \mid c$, then by (f), $a \mid bx, a \mid cy$. By (g), $a \mid bx + cy$.
- (i) If $a \mid b$, then $ax = b$ for some $x \in Z$. Thus $|a||x| = |ax| = |b| \Rightarrow |a| \leq$

$|b|$.

Congruences

Def 2.3.1: Let $a, b \in Z$ and $N \in Z$ with $N > 0$. Then a is congruent to b mod N, written $a \equiv b \pmod{N}$, if $N \mid a - b$.

Prop 2.3.1: Let $a, b, c, a', b' \in Z$ and $N, N' \geq 0$ be in Z.

- (a) Reflexivity: $a \equiv a \pmod{N}$
- (b) Symmetry: If $a \equiv b \pmod{N}$, then $b \equiv a \pmod{N}$
- (c) Transitivity: If $a \equiv b, b \equiv c \pmod{N}$, then $a \equiv c \pmod{N}$
- (d) Additivity: If $a \equiv b, a' \equiv b' \pmod{N}$, then $a + a' \equiv b + b' \pmod{N}$
- (e) Multiplicativity: If $a \equiv b, a' \equiv b' \pmod{N}$, then $aa' \equiv bb' \pmod{N}$
- (f) If $a \equiv b \pmod{NN'}$, then $a \equiv b \pmod{N}$

Prop 2.3.2: Let $a, N \in Z$ with $N > 0$. Let $q, r \in Z$ such that $a = Nq + r, 0 \leq r < N$. Then $a \equiv r \pmod{N}$.

Def 2.3.2: Let $a, N \in Z$ with $N > 0$. By Euclidean property of Z, $\exists$ unique q, r s.t. $a = Nq + r, 0 \leq r < N$. r is called "residue of a mod N" (remainder after division). Written as $a \bmod N$ or $r_N(a)$.

Example: For 15 mod 4, $15 = 4 \cdot 3 + 3$ where $0 \leq 3 < 4$. So $15 \equiv 3 \pmod{4}$ and residue $r_4(15) = 3$.

Warning: "mod" has two meanings:

- Relation: $a \equiv b \pmod{N}$
- Function: $a \bmod N = r$

Chapter 6

Congruences

Definition 6.0.1. Let $a, b \in \mathbb{Z}$ and $N \in \mathbb{Z}$ with $N > 0$. Then a is congruent to b mod N and we write

$$a \equiv b \pmod{N}$$

if $N \mid a - b$. In the above expression

$$a \equiv b \pmod{N}$$

we say that N is the modulus of the above relation between a and b.

Proposition 6.0.1. *Let $a, b, c, a', b' \in \mathbb{Z}$ and $N, N' \geq 0$ be in $\mathbb{Z}$.*

(a) Reflexivity: $a \equiv a \pmod{N}$
(b) Symmetry: *If* $a \equiv b \pmod{N}$, *then* $b \equiv a \pmod{N}$
(c) Transitivity: *If* $a \equiv b, b \equiv c \pmod{N}$, *then* $a \equiv c \pmod{N}$
(d) Additivity: *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $a + a' \equiv b + b' \pmod{N}$.
(e) Multiplicativity: *If* $a \equiv b$, $a' \equiv b' \pmod{N}$, *then* $aa' \equiv bb' \pmod{N}$.
(f) *If* $a \equiv b \pmod{NN'}$, *then* $a \equiv b \pmod{N}$

Proof. TODO □

The following connects the Euclidean property and the congruence relation:

Proposition 6.0.2. *Let $a, N \in \mathbb{Z}$ with $N > 0$. Let $q, r \in \mathbb{Z}$ such that*

$$a = Nq + r, \;\; 0 \leq r < N$$

Then $a \equiv r \pmod{N}$.

Proof. TODO

Definition 6.0.2. Let $a, N \in \mathbb{Z}$ with $N > 0$. By the Euclidean property of $\mathbb{Z}$, there exist unique q, r such that

$$a = Nq + r, \;\; 0 \leq r < N$$

r is called the "**residue** of a mod N" ("residue" = "what is left" after a is divided by N, i.e., the remainder after a is divided by N). It is common to write r as $a \bmod N$.

Sometimes $a \bmod N$ is written as $r_N(a)$. For instance to find the residue of $15 \bmod 4$, there is some q such that

$$15 = 4q + 3, \;\; 0 \leq 1 < 4$$

i.e.

$$15 \equiv 3 \pmod 4$$

where $0 \leq 1 < 4$. Therefore the residue of $15 \bmod 4$ is 1, or we simple write

$$15 \bmod 4 = 3$$

i.e., $r_4(15) = 3$.

Warning: "mod" now has two meanings. "mod N", where $N > 0$ is an integer, can be used to denote a relation between integers

$$a \equiv b \pmod N$$

and "mod N" can also be used to denote a function

$$a \bmod N = r$$

Chapter 7

Euclidean property

Thm 2.4.1: (Euclidean property) If $a, b \in Z$ with $b \neq 0$, then $\exists$ integers q, r s.t. $a = bq + r, 0 \leq |r| < |b|$

Thm 2.4.2: (Euclidean property 2) If $a, b \in Z$ with $b \neq 0$, then $\exists$ integers q, r s.t. $a = bq + r, 0 \leq r < |b|$

Thm 2.4.3: (Euclidean property 3) If $a, b \in Z$ with $a \geq 0, b > 0$, then $\exists$ integers $q \geq 0, r \geq 0$ s.t. $a = bq + r, 0 \leq r < b$

q = quotient, r = remainder, both unique. Computing $a, b \to q, r$ is division algorithm.

Python example:

```
a = 25
b = 8
q, r = divmod(25, 8)
print("%s = %s * %s + %s" % (a, b, q, r))
# Output: 25 = 8 * 3 + 1
```

If $a > 0, b > 0$: $q = \lfloor a/b \rfloor, r = a - bq$

Also: $a = b \cdot (a/b) + (a\%b)$ in programming terms.

To prove Euclidean property, we use Well-ordering principle:

WOP for $\mathbb{N}$: If $X \subseteq \mathbb{N}$ is non-empty, then X has least element.

WOP for Z: If $X \subseteq Z$ is non-empty and bounded below, then X has least element.

Note: $\mathbb{R}$ doesn't satisfy this. E.g., $(0, 1)$ has no minimum.

Proof of Thm 2.4.3: Assume $b > 0$. Let $X = \{a - bx | x \in Z, a - bx \geq 0\} \subseteq \mathbb{N} \cup \{0\}$. X non-empty since $a = a - b \cdot 0 \geq 0$ is in X. X is bounded below by 0. By WOP, X has minimal element r. So $r \in \mathbb{N} \cup \{0\}$ and $r = a - bq$ for some $q \in Z$.

Thus $a = bq + r, 0 \leq r$

Now prove $r < b$: Suppose $r \geq b$. Then $0 \leq r - b$ and: $a = bq + r = bq + (r - b + b) = b(q + 1) + (r - b)$

Therefore $a - b(q + 1) = (r - b) < r$

This means $a - b(q+1) \in X$ and smaller than $a - bq$, contradicting minimality of $a - bq$.

Also $q \geq 0$, otherwise $q < 0 \Rightarrow bq + r \leq b(-1) + r < 0$ since $r < b$.

Prop 2.4.1: The q, r in Thm 2.4.3 are unique.

Proof: If $a = bq + r = bq' + r'$ with $0 \leq r, r' < |b|$, then either $q = q'$ (thus $r = r'$) or assume $q > q'$. This gives $r' = b(q - q') + r > b + r \geq b$, contradicting $r' < b$.

Proof of Thm 2.4.1: Use Thm 2.4.3 for general case. Need to handle $a < 0$. Let $u = \pm 1$ so $ua \geq 0$ and $v = \pm 1$ so $vb > 0$. Note $u^{-1} = u, v^{-1} = v$. Let $a' = ua, b' = vb$.

By Thm 2.4.3, $\exists q' \geq 0, r'$ s.t. $a' = b'q' + r', 0 \leq r' < b'$, i.e., $ua = vbq' + r', 0 \leq r' < vb = |b|$

Multiply by u^{-1}: $a = uvbq' + ur', 0 \leq r' < vb = |b|$

Therefore $a = b(uvq') + ur', 0 \leq |ur'| < |b|$

With $q = uvq', r = ur'$, we get $a = bq + r, 0 \leq |r| < |b|$

Exercises:

- Ex 2.4.1: Prove Thm 2.4.3 using induction.
- Ex 2.4.2: Prove: If $a, b \in Z, b \neq 0$, then $\exists$ unique q, r s.t. $a = bq + r, b \leq r < 2b$.
- Ex 2.4.3: Prove every integer is congruent to 0, 1, 2, or 3 mod 4.
- Ex 2.4.4: Prove squares are 0 or 1 mod 4.

- Ex 2.4.5: Solve $4x^3 + y^2 = 5z^2 + 6$ in Z.
- Ex 2.4.6: Prove 11, 111, 1111,... are not perfect squares.
- Ex 2.4.7: How many of 3, 23, 123, 1123,... are perfect squares?

Solution to Ex 2.4.1: Prove by induction. Fix $b > 0$. Let $P(n)$ be: $\exists q, r$ s.t. $n = bq + r, 0 \leq r < b$

Base case $P(0)$: Set $q = 0, r = 0 \Rightarrow 0 = b \cdot 0 + 0, 0 \leq 0 < b$

Inductive step: Assume $P(n)$ holds, so $n = bq + r, 0 \leq r < b$. Then $n + 1 = bq + r + 1$.

Case 1: $r = b - 1$. Then $n + 1 = bq + (b - 1) + 1 = b(q + 1) + 0$. Set $q' = q + 1, r' = 0$.

Case 2: $r < b - 1$. Then $n + 1 = bq + (r + 1)$ with $0 \leq r + 1 < b$. Set $q' = q, r' = r + 1$.

Therefore $P(n + 1)$ holds in all cases. By induction, $P(n)$ holds for all $n \geq 0$.

202.4.1 To prove: For $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers q, r such that $a = bq + r$ and $b \leq r < 2b$.
Existence: By the standard division algorithm, we can find q_0, r_0 such that $a = bq_0 + r_0$ with $0 \leq r_0 < |b|$. If $r_0 \geq b$, then we already have $b \leq r_0 < 2b$, so set $q = q_0$ and $r = r_0$. If $r_0 < b$, then set $q = q_0 - 1$ and $r = r_0 + b$. Then $a = b(q_0 - 1) + (r_0 + b) = bq_0 + r_0 = a$, and $b \leq r_0 + b < 2b$.
Uniqueness: Suppose $a = bq_1 + r_1 = bq_2 + r_2$ with $b \leq r_1, r_2 < 2b$. Then $b(q_1 - q_2) = r_2 - r_1$. Both r_1 and r_2 are between b and $2b$, so $|r_2 - r_1| < b$. Since b divides $r_2 - r_1$ and $|r_2 - r_1| < b$, we must have $r_2 - r_1 = 0$, which implies $r_2 = r_1$ and $q_1 = q_2$.

202.4.2 To prove: Every integer is congruent to 0, 1, 2, or 3 modulo 4.
By the division algorithm, for any integer n, there exist integers q and r such that $n = 4q + r$ with $0 \leq r < 4$. This means $r \in \{0, 1, 2, 3\}$, so $n \equiv r \pmod 4$. Therefore, every integer is congruent to either 0, 1, 2, or 3 modulo 4.

202.4.3 To prove: If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 4$.
Any integer a is congruent to 0, 1, 2, or 3 modulo 4. Let's check each case: If $a \equiv 0 \pmod 4$, then $a^2 \equiv 0^2 \equiv 0 \pmod 4$. If $a \equiv 1 \pmod 4$, then $a^2 \equiv 1^2 \equiv 1 \pmod 4$. If $a \equiv 2 \pmod 4$, then $a^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod 4$. If $a \equiv 3 \pmod 4$, then $a^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 4$.
Therefore, any square is congruent to either 0 or 1 modulo 4.

202.4.4 To solve: $4x^3 + y^2 = 5z^2 + 6$ in $\mathbb{Z}$.

Taking modulo 4: $4x^3 + y^2 \equiv 5z^2 + 6 \pmod 4$ $0 + y^2 \equiv z^2 + 2 \pmod 4$ $y^2 \equiv z^2 + 2 \pmod 4$
From the previous exercise, $z^2 \equiv 0$ or $1 \pmod 4$, so: If $z^2 \equiv 0 \pmod 4$, then $y^2 \equiv 2 \pmod 4$ If $z^2 \equiv 1 \pmod 4$, then $y^2 \equiv 3 \pmod 4$
But we proved that $y^2 \equiv 0$ or $1 \pmod 4$, which contradicts both cases. Therefore, the equation has no integer solutions.

202.4.6 To determine which of $3, 23, 123, 1123, 11123, 111123, 1111123, ...$ are perfect squares.
Let's denote $T_n = 3$ if $n = 1$ and $T_n = \underbrace{11...1}_{n-1 \text{ digits}}\ 3$ for $n \geq 2$.
The numbers in our sequence are: $T_1 = 3$ $T_2 = 13$ $T_3 = 113$ $T_4 = 1113$ ...
None of these numbers end with 9, so none are perfect squares.
Alternatively, we can check modulo 4. For $n \geq 2$, we have: $T_n = 10^{n-1} + 10^{n-2} + ... + 10 + 3$
For odd n, $T_n \equiv 1 + 1 + ... + 1 + 3 \equiv 3 \pmod 4$ (odd number of 1's) For even n, $T_n \equiv 1 + 1 + ... + 1 + 3 \equiv 0 \pmod 4$ (even number of 1's)
When n is odd, $T_n \equiv 3 \pmod 4$, which cannot be a perfect square. When n is even, $T_n \equiv 0 \pmod 4$, so we need to check if $T_n/4$ is a perfect square.

Chapter 8

Bézout's identity and the Extended Euclidean Algorithm

Definition of GCD Let $a, b \in \mathbb{Z}$ s.t. not both a, b are 0. $d \in \mathbb{Z}, d \neq 0$ is common divisor of a, b if $d \mid a$ and $d \mid b$. $g \in \mathbb{Z}$ is greatest common divisor (gcd) of a, b if g is common divisor and largest among all common divisors. Note: If $a = b = 0$, gcd not defined (all integers are common divisors).

Bézout's Identity If $a, b \in \mathbb{Z}$ not both zero, then $\exists x, y \in \mathbb{Z}$ s.t. $\gcd(a, b) = ax + by$

x, y called Bézout coefficients (not unique).

Proof: Let $(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$ be linear combinations of a, b. Let $(g) = \{gx \mid x \in \mathbb{Z}\}$ be linear combinations of g.

Step 1: Show $\exists g > 0$ s.t. $(a, b) = (g)$

If $b = 0$, then $(a, 0) = (a)$ and done.

If $b \neq 0$, let u be unit s.t. $ub > 0$. The set $X = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\} \subseteq \mathbb{N}$ is non-empty (contains $0 \cdot a + ub$). By WOP, X has least element g.

Since $g \in X \subseteq (a, b)$, we have $(g) \subseteq (a, b)$.

To prove $(a, b) \subseteq (g)$, let $c \in (a, b)$, i.e., $c = ax + by$ for some $x, y \in \mathbb{Z}$. By Euclidean property, $\exists q, r \in \mathbb{Z}$ s.t. $c = gq + r, 0 \leq |r| < |g|$. Since $g > 0$, $0 \leq |r| < g$.

Need to show $r = 0$. Let u be unit s.t. $ur \geq 0$. Thus $0 \leq ur < g$ and $uc = ugq + ur$.

Suppose $r \neq 0 \Rightarrow ur > 0$. Then $ur = uc - ugq \in (a, b)$ since $c, g \in (a, b)$. Hence $ur \in X$ with $ur < g$, contradiction to minimality of g. Thus $r = 0$, so $c = gq \in (g)$.

Therefore $(a, b) = (g)$.

Step 2: Show $g = \gcd(a, b)$

Since $(a, b) = (g)$, $a \in (g)$ so $g \mid a$. Similarly $g \mid b$, so g is common divisor.

Since $(g) = (a, b)$, $g = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$. If $d \mid a$ and $d \mid b$, then $d \mid g$ by linearity. Thus $|d| \leq g$, making g the largest common divisor.

Extended Euclidean Algorithm To find x, y s.t. $\gcd(a, b) = ax + by$:

Example: Compute $\gcd(514, 24)$ and coefficients.

$$514 = 21 \cdot 24 + 10 \tag{8.1}$$
$$24 = 2 \cdot 10 + 4 \tag{8.2}$$
$$10 = 2 \cdot 4 + 2 \tag{8.3}$$
$$4 = 2 \cdot 2 + 0 \tag{8.4}$$

From $10 = 514 - 21 \cdot 24$, obtain $514 \cdot 1 + 24 \cdot (-21) = 10$.

From $4 = 24 - 2 \cdot 10 = 24 - 2(514 - 21 \cdot 24) = 514 \cdot (-2) + 24 \cdot 43$.

From $2 = 10 - 2 \cdot 4 = (514 - 21 \cdot 24) - 2(514 \cdot (-2) + 24 \cdot 43) = 514 \cdot 5 + 24 \cdot (-107)$.

Therefore $\gcd(514, 24) = 2 = 514 \cdot 5 + 24 \cdot (-107)$.

Systematic Algorithm Recursive process using remainders r_i:

$$r_0 = q_1 r_1 + r_2 \quad (r_0 = a, r_1 = b) \tag{8.5}$$
$$r_1 = q_2 r_2 + r_3 \tag{8.6}$$
$$\vdots \tag{8.7}$$
$$r_{n-2} = q_{n-1} r_{n-1} + r_n \tag{8.8}$$
$$r_{n-1} = q_n r_n + 0 \tag{8.9}$$

With backward substitution, track coefficients for r_0 and r_1.

Python Implementation

```
def EEA(a, b):
    """Extended Euclidean Algorithm
    Returns (r, c, d) where r = gcd(a, b) = c*a + d*b"""
    a0, b0 = a, b
    d0, d = 0, 1
    c0, c = 1, 0
    q = a0 // b0
    r = a0 - q * b0
    while r > 0:
        d, d0 = d0 - q * d, d
        c, c0 = c0 - q * c, c
        a0, b0 = b0, r
        q = a0 // b0
        r = a0 - q * b0
    r = b0
    return r, c, d
```

Exercise Solutions

Exercise 2.5.5 - Computing gcd and Bézout's coefficients:

1. $\gcd(0, 10) = 10$ since any non-zero integer divides 0. Bézout coefficients: $0 \cdot 0 + 1 \cdot 10 = 10$, so $x = 0, y = 1$.

2. $\gcd(10, 0) = 10$ similarly. Bézout coefficients: $1 \cdot 10 + 0 \cdot 0 = 10$, so $x = 1, y = 0$.

3. $\gcd(10, 1) = 1$ since 1 divides any integer.

$$10 = 10 \cdot 1 + 0 \tag{8.10}$$

Bézout coefficients: $0 \cdot 10 + 1 \cdot 1 = 1$, so $x = 0, y = 1$.

4. $\gcd(10, 10) = 10$.

$$10 = 1 \cdot 10 + 0 \tag{8.11}$$

Bézout coefficients: $1 \cdot 10 + 0 \cdot 10 = 10$, so $x = 1, y = 0$.

5. $\gcd(107, 5) = 1$.

$$107 = 21 \cdot 5 + 2 \tag{8.12}$$
$$5 = 2 \cdot 2 + 1 \tag{8.13}$$
$$2 = 2 \cdot 1 + 0 \tag{8.14}$$

From $5 = 2 \cdot 2 + 1$, get $1 = 5 - 2 \cdot 2$. From $107 = 21 \cdot 5 + 2$, get $2 = 107 - 21 \cdot 5$. Substituting: $1 = 5 - 2 \cdot (107 - 21 \cdot 5) = 5 - 2 \cdot 107 + 42 \cdot 5 = 43 \cdot 5 - 2 \cdot 107$. So $x = -2, y = 43$.

6. $\gcd(107, 26) = 1$.

$$107 = 4 \cdot 26 + 3 \tag{8.15}$$
$$26 = 8 \cdot 3 + 2 \tag{8.16}$$
$$3 = 1 \cdot 2 + 1 \tag{8.17}$$
$$2 = 2 \cdot 1 + 0 \tag{8.18}$$

From $3 = 1 \cdot 2 + 1$, get $1 = 3 - 1 \cdot 2$. From $26 = 8 \cdot 3 + 2$, get $2 = 26 - 8 \cdot 3$. Substituting: $1 = 3 - 1 \cdot (26 - 8 \cdot 3) = 9 \cdot 3 - 1 \cdot 26$. From $107 = 4 \cdot 26 + 3$, get $3 = 107 - 4 \cdot 26$. Substituting: $1 = 9 \cdot (107 - 4 \cdot 26) - 1 \cdot 26 = 9 \cdot 107 - 37 \cdot 26$. So $x = 9, y = -37$.

Exercise 2.5.6: Prove that if $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof: Since $\gcd(a, b) = 1$, by Bézout's identity, $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = 1$. Multiply both sides by c: $axc + byc = c$. Since $a \mid c$, $\exists m \in \mathbb{Z}$ s.t. $c = am$. So $axc = ax(am) = a^2xm$. Since $b \mid c$, $\exists n \in \mathbb{Z}$ s.t. $c = bn$. So $byc = by(bn) = b^2yn$. Thus $c = axc + byc = a^2xm + b^2yn$.

Now, since $\gcd(a, b) = 1$, we know a and b share no common factors. Since $a \mid c$ and $b \mid c$, by fundamental properties of divisibility in a unique factorization domain, we must have $ab \mid c$. This can also be seen because $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)} = ab$ when $\gcd(a, b) = 1$.

Exercise 2.5.7: Prove that if $a \mid c$, $b \mid c$, then $\frac{ab}{\gcd(a,b)} \mid c$.

Proof: Let $d = \gcd(a, b)$. Then $a = da'$ and $b = db'$ where $\gcd(a', b') = 1$. Since $a \mid c$, $\exists m \in \mathbb{Z}$ s.t. $c = am = da'm$. Since $b \mid c$, $\exists n \in \mathbb{Z}$ s.t. $c = bn = db'n$.

So $a' \mid \frac{c}{d}$ and $b' \mid \frac{c}{d}$. Since $\gcd(a', b') = 1$, by Exercise 2.5.6, $a'b' \mid \frac{c}{d}$.

Thus $\exists k \in \mathbb{Z}$ s.t. $\frac{c}{d} = a'b'k$, which gives $c = da'b'k = \frac{ab}{d}k$. Therefore $\frac{ab}{\gcd(a,b)} \mid c$.

Exercise 2.5.2: Using Extended Euclidean Algorithm, compute x, y such that $210x + 78y = \gcd(210, 78)$.

$$210 = 2 \cdot 78 + 54 \tag{8.19}$$
$$78 = 1 \cdot 54 + 24 \tag{8.20}$$
$$54 = 2 \cdot 24 + 6 \tag{8.21}$$
$$24 = 4 \cdot 6 + 0 \tag{8.22}$$

So $\gcd(210, 78) = 6$.

From $54 = 210 - 2 \cdot 78$, we get $210 \cdot 1 + 78 \cdot (-2) = 54$. From $24 = 78 - 1 \cdot 54 = 78 - 1 \cdot (210 - 2 \cdot 78) = 78 - 210 + 2 \cdot 78 = 210 \cdot (-1) + 78 \cdot 3$. From $6 = 54 - 2 \cdot 24 = (210 - 2 \cdot 78) - 2 \cdot (210 \cdot (-1) + 78 \cdot 3) = 210 - 2 \cdot 78 - 2 \cdot (-210) - 2 \cdot 3 \cdot 78 = 210 \cdot 3 + 78 \cdot (-8)$.

Therefore, $\gcd(210, 78) = 6 = 210 \cdot 3 + 78 \cdot (-8)$, so $x = 3$ and $y = -8$.

Exercise 2.5.4 (Water Jug Problem): Given jugs with capacities a and b, determine if target c is measurable.

Solution: c is measurable if and only if: 1. $c \leq \max(a, b)$ (cannot measure more than largest jug) 2. c is a multiple of $\gcd(a, b)$ (can only measure multiples of gcd)

This is because by Bézout's identity, we can find x, y such that $ax + by = \gcd(a, b)$. By repeating operations, we can measure any multiple of $\gcd(a, b)$ up to the capacity of the largest jug.

If $c > a + b$, it's impossible as we can't hold more than the combined capacity of both jugs.

Chapter 9

Euclidean algorithm – GCD

GCD Calculation via Euclidean Property

Given Euclidean property: $a = bq + r, 0 \leq r < b$

GCD Lemma: If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

Proof: Let d be any common divisor of a and b. Then $d \mid a$ and $d \mid b$, so $d \mid (a - bq) = r$. Thus, d is also a common divisor of b and r.

Conversely, if d is a common divisor of b and r, then $d \mid b$ and $d \mid r$, so $d \mid (bq + r) = a$. Thus, d is also a common divisor of a and b.

Since common divisors of (a, b) and (b, r) are identical, $\gcd(a, b) = \gcd(b, r)$.

Euclidean Algorithm:

```
ALGORITHM: GCD
INPUTS: a, b
OUTPUT: gcd(a, b)
if b == 0:
    return a
else:
    return GCD(b, a % b)
```

Example: $\gcd(514, 24)$

$$\begin{aligned}\gcd(514, 24) &= \gcd(24, 514 \bmod 24) = \gcd(24, 10) && (9.1)\\ &= \gcd(10, 24 \bmod 10) = \gcd(10, 4) && (9.2)\\ &= \gcd(4, 10 \bmod 4) = \gcd(4, 2) && (9.3)\\ &= \gcd(2, 4 \bmod 2) = \gcd(2, 0) && (9.4)\\ &= 2 && (9.5)\end{aligned}$$

Lamé's Theorem (1844): Let $a > b > 0$. If Euclidean algorithm takes n steps to compute $\gcd(a, b)$, then: 1. $a \geq F_{n+2}$ and $b \geq F_{n+1}$, where F_n is the n-th Fibonacci number 2. n is at most 5 times the number of digits in b

Proof Sketch: (a) By induction: If Euclidean algorithm takes n steps, then:

$$a \geq F_{n+2} \quad (9.6)$$
$$b \geq F_{n+1} \quad (9.7)$$

(b) Since $b \geq F_{n+1} \geq \phi^{n-1}$ (where $\phi = \frac{1+\sqrt{5}}{2}$), $\log_\phi b \geq n-1$, so $n \leq 5 \log_{10} b + 1 \leq 5\lfloor \log_{10} b + 1 \rfloor$

Result: Number of steps $\leq 5\times$ number of digits in b.

Proposition: Number of digits in b is $\lfloor \log_{10} b + 1 \rfloor$

Solutions to Exercises:

Exercise 2.6.3 - Compute using Euclidean Algorithm:

(a) $\gcd(10, 1)$

$$\gcd(10, 1) = \gcd(1, 10 \bmod 1) = \gcd(1, 0) = 1 \quad (9.8)$$

(b) $\gcd(10, 10)$

$$\gcd(10, 10) = \gcd(10, 0) = 10 \quad (9.9)$$

(c) $\gcd(107, 5)$

$$\begin{aligned}\gcd(107, 5) &= \gcd(5, 107 \bmod 5) = \gcd(5, 2) && (9.10)\\ &= \gcd(2, 5 \bmod 2) = \gcd(2, 1) && (9.11)\\ &= \gcd(1, 2 \bmod 1) = \gcd(1, 0) = 1 && (9.12)\end{aligned}$$

(d) $\gcd(107, 26)$

$$\begin{aligned}\gcd(107, 26) &= \gcd(26, 107 \bmod 26) = \gcd(26, 3) && (9.13)\\ &= \gcd(3, 26 \bmod 3) = \gcd(3, 2) && (9.14)\\ &= \gcd(2, 3 \bmod 2) = \gcd(2, 1) && (9.15)\\ &= \gcd(1, 2 \bmod 1) = \gcd(1, 0) = 1 && (9.16)\end{aligned}$$

(e) $\gcd(84, 333)$

$$\begin{aligned}\gcd(84, 333) &= \gcd(333, 84) \quad (\text{swap for } a \geq b) && (9.17)\\ &= \gcd(84, 333 \bmod 84) = \gcd(84, 81) && (9.18)\\ &= \gcd(81, 84 \bmod 81) = \gcd(81, 3) && (9.19)\\ &= \gcd(3, 81 \bmod 3) = \gcd(3, 0) = 3 && (9.20)\end{aligned}$$

Exercise 2.6.4 - Compute and simplify:

(a) $\gcd(ab, b)$

$$\gcd(ab, b) = \gcd(b, ab \bmod b) = \gcd(b, 0) = b \tag{9.21}$$

(b) $\gcd(a, a + 1)$

$$\begin{aligned}\gcd(a, a + 1) &= \gcd(a + 1, a \bmod (a + 1)) = \gcd(a + 1, a) && (9.22)\\ &= \gcd(a, a + 1 \bmod a) = \gcd(a, 1) && (9.23)\\ &= \gcd(1, a \bmod 1) = \gcd(1, 0) = 1 && (9.24)\end{aligned}$$

(c) $\gcd(ab + a, b)$ where $0 < a < b$

$$\begin{aligned}\gcd(ab + a, b) &= \gcd(b, (ab + a) \bmod b) && (9.25)\\ &= \gcd(b, a) \quad (\text{since } (ab + a) \bmod b = a) && (9.26)\end{aligned}$$

(d) $\gcd(a(a+1)+a, a+1)$ where $0 < a < a+1$

$$\begin{aligned}
\gcd(a(a+1)+a, a+1) &= \gcd(a+1, (a(a+1)+a) \bmod (a+1)) && (9.27)\\
&= \gcd(a+1, a(a+1) \bmod (a+1) + a \bmod (a+1)) && (9.28)\\
&= \gcd(a+1, 0+a) = \gcd(a+1, a) && (9.29)\\
&= \gcd(a, a+1 \bmod a) = \gcd(a, 1) && (9.30)\\
&= \gcd(1, a \bmod 1) = \gcd(1, 0) = 1 && (9.31)
\end{aligned}$$

(e) $\gcd(1 + x + \cdots + x^n, x)$

$$\begin{aligned}
\gcd(1 + x + \cdots + x^n, x) &= \gcd(x, (1 + x + \cdots + x^n) \bmod x) && (9.32)\\
&= \gcd(x, 1) \quad (\text{since } x \text{ divides } x + x^2 + \cdots + x^n) && (9.33)\\
&= \gcd(1, x \bmod 1) = \gcd(1, 0) = 1 && (9.34)
\end{aligned}$$

(f) $\gcd(F_{10}, F_{11})$ where F_n is the Fibonacci sequence

Using the Fibonacci recursion $F_{n+2} = F_{n+1} + F_n$, we have: $F_{11} = F_{10} + F_9$, so $F_9 = F_{11} - F_{10}$

$$\begin{aligned}
\gcd(F_{10}, F_{11}) &= \gcd(F_{11}, F_{10} \bmod F_{11}) && (9.35)\\
&= \gcd(F_{11}, F_{10}) && (9.36)\\
&= \gcd(F_{10}, F_{11} \bmod F_{10}) && (9.37)\\
&= \gcd(F_{10}, F_9) \quad (\text{since } F_{11} \bmod F_{10} = F_9) && (9.38)
\end{aligned}$$

Continuing this pattern: $\gcd(F_{10}, F_9) = \gcd(F_9, F_8) = \cdots = \gcd(F_2, F_1) = \gcd(1, 1) = 1$

Thus, $\gcd(F_{10}, F_{11}) = 1$

More generally, $\gcd(F_n, F_{n+1}) = 1$ for any $n \geq 1$.

Exercise 2.6.6 - Number of subarrays with GCD equal to k:

Approach: 1. For each start index i, compute the running GCD of elements from index i to index j. 2. Count how many times this running GCD equals k.

```
def subarrayGCD(nums, k):
    count = 0
    n = len(nums)

    for i in range(n):
        # Initialize gcd as the first element in current subarray
        current_gcd = nums[i]

        # If this single element equals k, count it
        if current_gcd == k:
            count += 1

        # Try expanding subarray by adding elements
        for j in range(i+1, n):
            # Update running GCD
            current_gcd = math.gcd(current_gcd, nums[j])

            # If GCD equals k, count this subarray
            if current_gcd == k:
                count += 1

            # If GCD becomes less than k, no need to continue
            # as adding more elements can't increase GCD
            if current_gcd < k:
                break

    return count
```

Exercise 2.6.7 - GCD Sort: Problem: Can we sort an array by only swapping pairs where gcd ¿ 1?

Solution: We need to determine if elements can be moved to their correct sorted positions.

Key insight: Elements that share factors ¿ 1 can be connected, forming "connected components". Elements in the same component can be rearranged freely.

```
def gcdSort(nums):
    Find maximum value to set up DSU
    max_val = max(nums)
```

```
    Create DSU for potential values
    parent = list(range(max_val + 1))

    def find(x):
        if parent[x] != x:
            parent[x] = find(parent[x])
        return parent[x]

    def union(x, y):
        parent[find(x)] = find(y)

    Step 1: Connect numbers with their prime factors
    for num in nums:
        temp = num
        # Try potential factors from 2 to sqrt(num)
        i = 2
        while i * i <= temp:
            if temp % i == 0:
                # Union num with its factor i
                union(num, i)
                while temp % i == 0:
                    temp //= i
            i += 1
         If temp > 1, it's a prime factor
        if temp > 1:
            union(num, temp)

     Step 2: Check if sorted array can be achieved
    sorted_nums = sorted(nums)
    for i in range(len(nums)):
        if find(nums[i]) != find(sorted_nums[i]):
            return False

    return True
```

202.5.1 a) $\gcd(0, 10)$: Since one number is 0, $\gcd(0, 10) = 10$
b) $\gcd(10, 0)$: Since one number is 0, $\gcd(10, 0) = 10$
c) $\gcd(10, 1)$: Since one number is 1, $\gcd(10, 1) = 1$
d) $\gcd(10, 10)$: When numbers are equal, $\gcd(10, 10) = 10$

e) $\gcd(107, 5)$: $107 = 5 \cdot 21 + 2$ $5 = 2 \cdot 2 + 1$ $2 = 1 \cdot 2 + 0$ Therefore, $\gcd(107, 5) = 1$

f) $\gcd(107, 26)$: $107 = 26 \cdot 4 + 3$ $26 = 3 \cdot 8 + 2$ $3 = 2 \cdot 1 + 1$ $2 = 1 \cdot 2 + 0$ Therefore, $\gcd(107, 26) = 1$

g) $\gcd(84, 333)$: $333 = 84 \cdot 3 + 81$ $84 = 81 \cdot 1 + 3$ $81 = 3 \cdot 27 + 0$ Therefore, $\gcd(84, 333) = 3$

h) $\gcd(F_{10}, F_{11})$: $F_{10} = 55$, $F_{11} = 89$ $89 = 55 \cdot 1 + 34$ $55 = 34 \cdot 1 + 21$ $34 = 21 \cdot 1 + 13$ $21 = 13 \cdot 1 + 8$ $13 = 8 \cdot 1 + 5$ $8 = 5 \cdot 1 + 3$ $5 = 3 \cdot 1 + 2$ $3 = 2 \cdot 1 + 1$ $2 = 1 \cdot 2 + 0$ Therefore, $\gcd(F_{10}, F_{11}) = 1$

i) $\gcd(ab, b)$: $ab = b \cdot a + 0$ Therefore, $\gcd(ab, b) = b$

j) $\gcd(a, a+1)$: $a+1 = a \cdot 1 + 1$ $a = 1 \cdot a + 0$ Therefore, $\gcd(a, a+1) = 1$

k) $\gcd(ab + a, b)$ where $0 < a < b$: $ab + a = b \cdot a + a = a(b + 1)$ $\gcd(a(b + 1), b) = \gcd(a, b) \cdot \gcd(b + 1, b) = \gcd(a, b) \cdot 1 = \gcd(a, b)$ Therefore, $\gcd(ab + a, b) = \gcd(a, b)$

l) $\gcd(a(a + 1) + a, a + 1)$ where $0 < a$: $a(a + 1) + a = a(a + 1 + 1) = a(a+2)$ $\gcd(a(a+2), a+1) = \gcd(a, a+1) \cdot \gcd(a+2, a+1) = 1 \cdot 1 = 1$ Therefore, $\gcd(a(a + 1) + a, a + 1) = 1$

Chapter 10

Primes

Definition of Prime A prime p is a positive integer > 1 that is divisible only by 1 and itself. Examples: 2, 3, 5, 7, 11, 13, 17, 19, ...

Classification of Integers

- 0 - zero element
- 1 - unit element (only invertible element ≥ 0)
- primes - 2, 3, 5, 7, 11, ...
- composites - integers > 1 which are not primes

Euclid's Lemma If p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: Assume $p \nmid a$ (otherwise done). Since $\gcd(a, p) \mid p$ and p is prime, $\gcd(a, p) = 1$. By Bézout's identity, $\exists x, y \in \mathbb{Z}$ such that $ax + py = 1$. Multiply by b: $abx + pby = b$ Since $p \mid ab$ and $p \mid pb$, we have $p \mid b$.

Corollary If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for at least one i.

Proof: By strong induction. Base case $n = 2$ is Euclid's lemma. Inductive step: If $p \mid a_1 a_2 \cdots a_n a_{n+1}$, let $b = a_n a_{n+1}$. Then $p \mid a_1 a_2 \cdots a_{n-1} b$. By induction, p divides at least one of $a_1, ..., a_{n-1}, b$. If $p \mid b = a_n a_{n+1}$, then by Euclid's lemma, $p \mid a_n$ or $p \mid a_{n+1}$. Therefore $p \mid a_i$ for at least one $i \in \{1, 2, ..., n+1\}$.

Fundamental Theorem of Arithmetic Every positive integer > 1 can be written as a unique product of primes (up to permutation).

Proof: (a) Existence: By induction on $n \geq 2$. Base: $n = 2$ is prime, so it's a product of itself. Inductive step: For $n + 1$, either: - $n + 1$ is prime (done) - $n + 1$ is composite: $n + 1 = dm$ where $1 < d, m < n + 1$ By induction, $d = p_1 \cdots p_k$ and $m = q_1 \cdots q_l$ So $n + 1 = p_1 \cdots p_k q_1 \cdots q_l$

(b) Uniqueness: If $p_1 \cdots p_m = q_1 \cdots q_n$ where primes are in ascending order: - $p_1 \mid q_1 \cdots q_n$, so by Euclid's lemma, $p_1 \mid q_i$ for some i - Since q_i is prime, $p_1 = q_i$ - Since primes are arranged in ascending order, $p_1 = q_1$ - Cancelling: $p_2 \cdots p_m = q_2 \cdots q_n$ - Continue this process to get $m = n$ and $p_i = q_i$ for all i

Properties of Prime Factorization Let $a = \prod_{p \in P} p^{a_p}$, $b = \prod_{p \in P} p^{b_p}$, $c = \prod_{p \in P} p^{c_p}$ where P is a finite set of primes.

- (a) $c = ab \implies c_p = a_p + b_p$
- (b) $a \mid b \implies a_p \leq b_p$ for all $p \in P$
- (c) $c = \gcd(a, b) \implies c_p = \min(a_p, b_p)$
- (d) $c = \text{lcm}(a, b) \implies c_p = \max(a_p, b_p)$
- (e) $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$

Bound on Prime Factors If $n > 1$ is not prime, then there is a prime factor p such that $p \leq \sqrt{n}$.

Brute-Force Primality Test

```
def is_prime(n):
    if n < 2:
        return False
    d = 2
    while d*d <= n:  # d <= sqrt(n)
        if n % d == 0:
            return False
        d += 1
    return True
```

Runtime: $O(\sqrt{n})$ with respect to value, $O(2^{b/2})$ for b bits (exponential).

Exercise Solutions

Exercise 2.7.1: Prove there are infinitely many composites.

Proof: For any $n \geq 4$, consider $n!$ (factorial). $n! = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1$ $n! \geq n \geq 4$, so $n! > 1$. Also, for any k where $2 \leq k \leq n$, we have $k \mid n!$. So $n!$ has multiple divisors and is therefore composite. Since we can construct a unique composite $n!$ for every $n \geq 4$, there are infinitely many composites.

Exercise 2.7.2: Prove there are infinitely many primes of form $4k + 3$.

Proof: Assume there are finitely many primes of the form $4k+3$: $p_1, p_2, \ldots, p_r$.

Let $N = 4p_1p_2 \cdots p_r - 1 = 4M - 1$ where $M = p_1p_2 \cdots p_r$. Note that $N \equiv 3 \pmod 4$.

Now, N must have a prime factor. Let q be any prime factor of N.

If $q \equiv 1 \pmod 4$, then $q \mid N$ implies $q \mid 4M - 1$. Since $q \equiv 1 \pmod 4$, we have $q = 4t + 1$ for some t. But then $q \mid 4M - 1$ implies $(4t + 1) \mid (4M - 1)$, which means $(4t + 1) \mid (4M - (4t + 1))$, so $(4t + 1) \mid (4(M - t) - 2)$. This means $(4t + 1) \mid 2$, which is impossible since $q = 4t + 1 \geq 5$.

Therefore, any prime factor q of N must be of the form $4k+3$. But this means q is one of $p_1, p_2, \ldots, p_r$. So $q \mid p_1p_2 \cdots p_r$, which means $q \mid M$.

Now we have: - $q \mid N = 4M-1$ - $q \mid 4M$ This implies $q \mid (4M-1)-4M = -1$, which is impossible for a prime.

Therefore, our assumption was wrong: there are infinitely many primes of the form $4k + 3$.

Exercise 2.7.10: Count Primes (LeetCode 204)

Sieve of Eratosthenes algorithm:

```
def countPrimes(n):
    if n <= 2:
        return 0

    # Initialize array with all numbers potentially prime
    isPrime = [True] * n
    isPrime[0] = isPrime[1] = False

    # Sieve algorithm
    for i in range(2, int(n**0.5) + 1):
        if isPrime[i]:
            # Mark all multiples as non-prime
            for j in range(i*i, n, i):
                isPrime[j] = False

    # Count primes
    return sum(isPrime)
```

Time complexity: $O(n \log \log n)$ Space complexity: $O(n)$

Exercise 2.7.11: Perfect Number (LeetCode 507)

```
def checkPerfectNumber(num):
    if num <= 1:
        return False

    # Sum of divisors starts with 1
    sum_divisors = 1

    # Check divisors up to sqrt(num)
    for i in range(2, int(num**0.5) + 1):
        if num % i == 0:
            # Add both i and num/i to sum
            sum_divisors += i
            if i != num // i:  # Avoid counting sqrt(num) twice
                sum_divisors += num // i

    return sum_divisors == num
```

Perfect numbers (for verification): 6, 28, 496, 8128, ...

Exercise 2.7.18: Greatest Common Divisor of Strings (LeetCode 1071)

```
def gcdOfStrings(str1, str2):
    # If concatenation in both orders is not the same, no GCD exists
    if str1 + str2 != str2 + str1:
        return ""

    # GCD length is the GCD of the lengths
    def gcd(a, b):
        while b:
            a, b = b, a % b
        return a

    gcd_len = gcd(len(str1), len(str2))
    return str1[:gcd_len]
```

Time complexity: $O(n)$ where n is the length of the longer string Space complexity: $O(n)$ for string operations

Exercise 2.7.19: Euler's Prime-Generating Polynomial

$P(x) = x^2 - x + 41$ generates primes for $x = 0, 1, 2, ..., 40$.

Verification for a few values: - $P(0) = 0^2 - 0 + 41 = 41$ (prime) - $P(1) = 1^2 - 1 + 41 = 41$ (prime) - $P(2) = 2^2 - 2 + 41 = 43$ (prime) - $P(3) = 3^2 - 3 + 41 = 47$ (prime)

$P(40) = 40^2 - 40 + 41 = 1600 - 40 + 41 = 1601$ (prime) $P(41) = 41^2 - 41 + 41 = 1681 = 41^2$ (composite)

Euler lucky numbers are values of n where $x^2 - x + n$ produces primes for all $0 \leq x < n$. Examples include 2, 3, 5, 11, 17, and 41.

Exercise 2.7.20: Polynomials Can't Always Generate Primes

Proof: Let $P(x)$ be a non-constant polynomial.

For any prime p, let's consider values of $P(x)$ modulo p. Since there are only p possible remainders when dividing by p (namely $0, 1, 2, ..., p - 1$), by the Pigeonhole Principle, the sequence $P(0), P(1), P(2), ...$ must have values that repeat modulo p.

This means there exist distinct integers a and b such that $P(a) \equiv P(b) \pmod{p}$. Let $m = |b - a|$. Then $p \mid (P(a) - P(b))$.

Now, for any integer k, consider $P(a + km)$. By properties of polynomials, $P(a + km) \equiv P(a) \pmod{p}$ for all k.

Therefore, $p \mid P(a + kp)$ for all $k \geq 0$. But if $p \mid P(n)$, then $P(n)$ cannot be prime unless $P(n) = p$.

Since P is non-constant, there can be at most one value of n where $P(n) = p$. Therefore, there are infinitely many values n where $P(n)$ is composite.

Chapter 11

Euler's Totient Function

11.1 Definition and Basic Properties

For a positive integer n, Euler's totient function $\varphi(n)$ counts the positive integers up to n that are relatively prime to n. In other words:

$$\varphi(n) = |\{k : 1 \leq k \leq n, \gcd(k, n) = 1\}|$$

11.1.1 Elementary Values

- $\varphi(1) = 1$, since $\gcd(1, 1) = 1$.
- For a prime p, $\varphi(p) = p-1$, since all numbers $1, 2, \ldots, p-1$ are relatively prime to p.
- For a prime power p^k, $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.

Multiplicativity

The Euler totient function is multiplicative, meaning if $\gcd(m, n) = 1$, then:

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

This property helps compute $\varphi(n)$ for any integer by using its prime factorization.

11.2 Computation Formula

If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of n, then:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

11.2.1 Proof

For a prime power p^a, the numbers not relatively prime to p^a are multiples of p: $p, 2p, 3p, \ldots, p^{a-1}p$. There are p^{a-1} such numbers, so:

$$\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right)$$

By multiplicativity, for $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$:

$$\varphi(n) = \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k})$$

$$= p_1^{a_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{a_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k} \left(1 - \frac{1}{p_k}\right)$$

$$= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Implementation

The following algorithm computes $\varphi(n)$ efficiently:

```
def euler_phi(n):
    result = n  # Initialize with n
    p = 2       # Start with the smallest prime

    while p * p <= n:  # Check up to sqrt(n)
        if n % p == 0: # If p is a factor
            while n % p == 0:
                n //= p # Divide out all instances of p
```

```
            result -= result // p  # Multiply by (1-1/p)
        p += 1

    # If n has a prime factor > sqrt(n)
    if n > 1:
        result -= result // n

    return result
```

11.3 Applications in Number Theory

11.3.1 Euler's Theorem

If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

This generalizes Fermat's Little Theorem, which states that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof Sketch

Consider the set of integers relatively prime to n: $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$. When we multiply each element by a (with $\gcd(a, n) = 1$), we get a permutation of the same set modulo n. Thus:

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n}$$

Simplifying:

$$a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n}$$

Since $\gcd(r_i, n) = 1$ for all i, we can cancel these factors to get $a^{\varphi(n)} \equiv 1 \pmod{n}$.

11.3.2 Application in Cryptography

Euler's theorem is fundamental in modular exponentiation, which is used in RSA cryptography:

- For a public key (n, e) and private key d, we have $e \cdot d \equiv 1 \pmod{\varphi(n)}$

- When encrypting a message m, we compute $c = m^e \bmod n$
- When decrypting, we compute $m = c^d \bmod n$
- The decryption works because $c^d = (m^e)^d = m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi(n)})^k \equiv m \cdot 1^k \equiv m \pmod{n}$

11.4 Properties and Formulas

11.4.1 Sum of Totient Values

For any positive integer n:

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

where the sum is over all positive divisors d of n.

Proof Idea

Consider the fractions $\frac{k}{n}$ for $1 \leq k \leq n$. When reduced to lowest terms, each becomes $\frac{j}{d}$ where $d|n$ and $\gcd(j, d) = 1$. For each divisor d of n, there are $\varphi(d)$ fractions with denominator d. Therefore, the total number of fractions is $\sum_{d|n} \varphi(d) = n$.

11.4.2 Möbius Inversion Formula

The Möbius inversion formula provides another way to express $\varphi(n)$:

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$$

where $\mu(d)$ is the Möbius function.

11.5 Extensions and Generalizations

11.5.1 Jordan's Totient Function

Jordan's totient function $J_k(n)$ counts the number of k-tuples of positive integers all $\leq n$ that form a coprime $(k+1)$-tuple together with n.

For $k = 1$, we recover Euler's totient function: $J_1(n) = \varphi(n)$.

Carmichael Function

The Carmichael function $\lambda(n)$ is the smallest positive integer such that:

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

for all integers a with $\gcd(a, n) = 1$.

It's always true that $\lambda(n)|\varphi(n)$, and they are equal when n is 1, 2, 4, a power of an odd prime, or twice a power of an odd prime.

11.5.2 Computational Complexity

Computing $\varphi(n)$ directly from its definition requires factoring n, which is computationally difficult for large numbers.

However, if the prime factorization is known, $\varphi(n)$ can be computed efficiently using the product formula.

202.13.1 To compute the smallest positive r such that $5^{642} \equiv r \pmod{640}$.
Using Euler's Theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$ for $\gcd(a, n) = 1$.
First, calculate $\phi(640)$: $640 = 2^7 \cdot 5$ $\phi(640) = \phi(2^7) \cdot \phi(5) = 2^6 \cdot 4 = 64 \cdot 4 = 256$
Since $\gcd(5, 640) = 5$, we can't directly apply Euler's Theorem. Let's write: $640 = 5 \cdot 128$
We need to find $5^{642} \bmod 640$. Note that $5^{642} = 5^2 \cdot 5^{640}$. $5^2 = 25$ $5^{640} = (5^{128})^5 = (5^{128})^5$
Since $\gcd(5, 128) = 1$, $5^{\phi(128)} \equiv 1 \pmod{128}$. $\phi(128) = \phi(2^7) = 2^6 = 64$
So $5^{64} \equiv 1 \pmod{128}$, which means $5^{128} \equiv 1 \pmod{128}$.
This gives us $5^{640} = (5^{128})^5 \equiv 1^5 \equiv 1 \pmod{128}$ Therefore, $5^{640} = 128k + 1$ for some integer k.
$5^{642} = 5^2 \cdot 5^{640} = 25 \cdot (128k + 1) = 25 + 3200k$ $5^{642} \bmod 640 = (25 + 3200k) \bmod 640 = 25 \bmod 640 = 25$
Therefore, $r = 25$.

202.13.2 To find $3^{123456789} \bmod 100$.
First, we determine $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(4) \cdot \phi(25) = 2 \cdot 20 = 40$.
Since $\gcd(3, 100) = 1$, by Euler's Theorem: $3^{40} \equiv 1 \pmod{100}$
To find $3^{123456789} \bmod 100$, we compute $123456789 = 40 \cdot 3086419 + 29$
So $3^{123456789} \equiv 3^{29} \pmod{100}$
Computing step by step: $3^1 = 3$ $3^2 = 9$ $3^4 = 81$ $3^8 \equiv 81^2 \equiv 61 \pmod{100}$ $3^{16} \equiv 61^2 \equiv 21 \pmod{100}$ $3^{24} = 3^{16} \cdot 3^8 \equiv 21 \cdot 61 \equiv 81 \pmod{100}$ $3^{25} = 3^{24} \cdot 3^1 \equiv 81 \cdot 3 \equiv 43 \pmod{100}$ $3^{29} = 3^{25} \cdot 3^4 \equiv 43 \cdot 81 \equiv 83 \pmod{100}$

Therefore, $3^{123456789} \bmod 100 = 83$.

202.13.3 The hundreds digit of $3^{123456789}$ is the digit in the hundreds place of this number.
Since $3^{123456789} \equiv 83 \pmod{100}$, we know $3^{123456789} = 100k + 83$ for some integer k.
To find the hundreds digit, we need the value of $\lfloor \frac{3^{123456789}}{100} \rfloor \bmod 10$.
We can compute $3^{123456789} \bmod 1000$ to find the first three digits.
Using $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(8) \cdot \phi(125) = 4 \cdot 100 = 400$:
$3^{400} \equiv 1 \pmod{1000}$
$123456789 = 400 \cdot 308641 + 389$
So $3^{123456789} \equiv 3^{389} \pmod{1000}$
Computing $3^{389} \bmod 1000$ step by step (similar to previous problem), we get $3^{389} \equiv 783 \pmod{1000}$.
Therefore, $3^{123456789} = 1000m + 783$ for some integer m.
The hundreds digit is $\lfloor \frac{783}{100} \rfloor \bmod 10 = 7$.