Week 8 - Monday

I) Integer Representation.

II) Modular Exponentiation.

III) Proving the uniqueness of FTA, and learning lots of powerful machinery and lemmas along the path
- → gcd
- → Euclid Alg
- → Bezout's Them
- → Euclid Lemma
- → Corrolary of Euclid's Lemma

IV) Recursive defn of functions.

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \leftrightarrow m \mid a-b$

Binary, base b representation

Representations of Integers (4.2)

THEOREM 1

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

- The representation of n given in Them 1 is called base b expansion of n.
- The base b expansion of n is denoted by $(a_k a_{k-1} \cdots a_0)_b$

Decimal Representation

In decimal, the number $d_k d_{k-1} \cdots d_0$ with $d_i \in \{0, 1, \ldots, 9\}$ for all i, refers to

$$d_0 + d_1 \times 10 + \cdots + d_k \times 10^k.$$

Proposition: Let $n \in \mathbb{Z}_{>0}$. have digits $d_k d_{k-1} \dots d_0$.
Then $9 \mid n$ iff $9 \mid d_k + d_{k-1} + \dots + d_0$.

$9 \nmid 1235$

Proof: Assume arbitrary integer n with decimal representation $d_k d_{k-1} \dots d_0$ Observe that $n = d_0 + 10 \times d_1 \times \dots \times 10^k d_k = \sum_{i=0}^{k} d_i \cdot 10^i$

Observe that $n \equiv \sum_{i=0}^{k} d_i 10^i \equiv d_0 + \sum_{i=1}^{k} d_i 10^i$.

Observe that $10^1 \equiv 1 \pmod 9$

$10^2 \equiv 6 \equiv 1 \pmod 9$

$\vdots$

$10^i \equiv 1 \pmod 9$

Hence, $n \equiv d_0 + \sum_{i=1}^{k} d_i \cdot (1) \equiv \sum_{i=0}^{k} d_i \pmod 9$

Hence, $9 \mid n \longleftrightarrow 9 \mid \sum_{i=0}^{k} d_i$

There Are Other Number Systems As Well

- $b=2$ is called binary, e.g.,

$(10101)_2 = 1\times2^5 + 1\times2^3 + 1\times2^2 + 0\times2^1 + 1 = 32+8+4+1 =$

- $b=8$ is called octal: 8 digits are required for octal expansion

e.g., $(721)_8 = 7\times8^2 + 2\times8 + 1$

- $b=16$ is hexadecimal, e.g., 16 digits are required (0, 1, .., 9, a, b, c, d, e, f)

10 ← 11 ← 1_2 13 14 15

e.g., $(1cd)_{16} = 1\times16^2 + 12\times16 + 13 =$

■ How to convert to base b expansion? For instance, $b=2$

$45 = 2\times 22 + 1$ ← rightmost digit

$22 = 2\times 11 + 0$

$11 = 2\times 5 + 1$

$5 = 2\times 2 + 1$

$2 = 2\times 1 + 0$

$1 = 2\times 0 + 1$ stop

$45 = (1\,0\,1\,1\,0\,1)_2$

$45 = 2\times 22 + 1 = 2\times(2\times 11 + 0) + 1$

$= 2\times(2\times(2\times 5 + 1) + 1 = \cdots$

remainders from top to bottom are the digits in the binary representation.

Find the hexadecimal expansion of 177130.

$177130 = 16 \cdot 11070 + 10$

$11070 = 16 \cdot 691 + 14$

$691 = 16 \cdot 43 + 3$

$43 = 16 \cdot 2 + 11$

$2 = 16 \cdot 0 + 2$

Hence, $177130 = (2b3ea)_{16}$

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

Repeated squaring
$5^{2024} \bmod 12$

Modular Exponentiation

Motivation: Consider the following problem: $3^{644} \bmod 645$.

$3^{644} \equiv ?$ (mod 645)

$3 \equiv 3$ (mod 645)

$3^2 \equiv 9$

$3^3 \equiv 27$

$3^4 \equiv 81$

$3^5 \equiv 243$

$3^6 \equiv 729 \equiv 84$

$3^7 \equiv 84 \times 3 \equiv 252$

$3^8 \equiv 252 \times 3 \equiv 756 \equiv 111$

$3^9 \equiv 3 \times 111$

In many cryptography applications, you need finding the answer to questions like $3^{644} \bmod 645$ very quickly.

We can find the answer quickly if we represent the exponent in binary. $644 = (1010000100)_2 = 2^9 + 2^7 + 2^2$.

$$3^{644} = 3^{2^2+2^7+2^9} = 3^{2^2} \times 3^{2^7} \times 3^{2^9}$$

Hence, $3^{644} \equiv (3^{2^2} \bmod 645) \times (3^{2^7} \bmod 645) \times (3^{2^9} \bmod 645)$

$3^{2^0} \equiv 3 \pmod{645}$

$3^{2^1} \equiv (3^{2^0})^2 \equiv 3^2 \pmod{645}$

$\vdots$

$(3^{2^{i+1}}) \equiv (3^{2^i})^2 \equiv (3^{2^i} \bmod 645)^2 \pmod{645}$

This idea is called Repeated Squaring (See "Alg 5" in 4.2)

Goal: find $b^n \bmod m$.

1. write n in binary representation $n = (a_{k-1} a_{k-2} \cdots a_0)_2$
2. Express b^n as $b^{2^{a_{k-1}}} \times b^{2^{a_{k-2}}} \times \cdots \times b^{2^{a_0}}$
3. Compute $(b^{2^0} \bmod m), \ldots, (b^{2^{a_{k-1}}} \bmod m)$
   by repeated squaring.
   $b_1^2 \equiv t_0 \pmod m$
   $b_2^2 \equiv t_0^2 \equiv t_1 \pmod m$
   $b^2 \equiv t_1^2 \equiv t_2 \pmod m$
   $\vdots$
4. plug into step 3.

So far:

Divisibility : $a|b$

Division Alg : $a = dq + r$, $0 \le r < d$

Congruence : $a \equiv b \pmod m$ if $a \bmod m = b \bmod m$.

Arithmetic mod m : $a+b \equiv (a \bmod m) + (b \bmod m) \pmod m$

$ab \equiv (a \bmod m)(b \bmod m) \pmod m$

Repeated Squaring : $b^{2^k} \equiv (b^{2^{k-1}})^2 \pmod m$

Next we will see:

Prime numbers; GCD ; Euclidean Alg.

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

Repeated squaring
$5^{2024} \bmod 12$

FTA: Existence and uniqueness

Prime Numbers

Defn: An integer $p > 1$ is prime if it has no divisors other than 1 and itself.

Formally: p is prime $\iff \forall k \in \mathbb{Z}_{>0}\ (k \mid p \to k = 1 \vee k = p)$

Defn: An integer $c > 1$ is composite if it is not prime, i.e., $c = ab$ for some integers $a, b \neq 1$.

Fundamental Theorem of Arithmetic (FTA)

Every integer $n>1$ can be written uniquely as a product of primes $p_1, p_2, \dots, p_k$ listed in non-decreasing order

Formal:

$$\forall n>1 \quad \exists! \, p_1,\dots,p_k \left(p_1,\dots p_k \text{ are prime} \wedge p_1 \leq p_2 \leq \dots \leq p_k \wedge n = p_1 \cdot p_2 \cdots p_k\right)$$

e.g.: $15 = 3 \cdot 5$ $\quad$ $24 = 2 \cdot 2 \cdot 2 \cdot 3$

Proof: We have already proved the existence part of the proof by strong induction. See W4-Friday notes. Today, we prove the uniqueness part.

(by use of GCD)

Before that let's take a fun detour: **The Infinitude of Primes**

(Euclid) Theorem: There are infinitely many prime numbers.

Proof:

Assume for contradiction there are finitely many primes.
Let $P = \{p_1, \dots, p_n\}$ denote the finite set of primes.
Consider $q = p_1 \times \dots \times p_n + 1$. Notice that $q \notin P$. Hence, q is not a prime, i.e., q is composite. Hence, by FTA there exists a prime number p_j such that $p_j \mid q$.
Observe that $p_j \mid p_1 \times \dots \times p_n$. Hence, $p_j \mid q - p_1 \dots p_n$. Thus, $p_j \mid 1$. which is a contradiction since p_j is a prime.

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

gcd(a,b),
Eclid Algorithm

Repeated squaring
$5^{2024} \bmod 12$

FTA: Existence and uniqueness

GCD

Defn: If a and b are integers, not both zero, then the greatest common divisor $\gcd(a,b)$ is the largest $d \in \mathbb{Z}_{>0}$ such that $d|a$ and $d|b$.

e.g.: $\gcd(10,36)$

- divisors of $10 = \{1, 2, 5, 10\}$
- divisors of $36 = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

Hence, $\gcd(10,36) = 2$

Euclidean Algorithm (to find gcd)

Key observation: If $a > b > 1$ and $a = bq + r$ where $0 \leq r < b$, then $\gcd(a,b) = \gcd(b,r)$

This observation is not obvious to see. In fact, it follows from the next lemma, which we will prove.

Lemma 1: If $a > b > 1$ and $a = bq + r$ and $0 < r < b$, then for any $d \in \mathbb{Z}_{>0}$, $(d|a \wedge d|b) \longleftrightarrow (d|b \wedge d|r)$.

what does this lemma mean?
The set of common divisor for a and b is the same as the set of common divisor for b and r. Hence, $\gcd(a,b) = \gcd(b,r)$

Proof of lemma 1:

($\rightarrow$) Assume arbitrary $a > b > 1$. Choose q and r s.t. $a = b \cdot q + r$ and $0 \leq r < b$. Assume that $d \in \mathbb{Z}_{>0}$ is a common divisor of a and b, i.e. $d \mid a$ and $d \mid b$. Observe that $d \mid a - bq$. Hence, $d \mid r$ as desired. $\square$

($\leftarrow$) Homework

Example. gcd(252, 198)

$252 = 1 \times 198 + 54$ $\quad gcd(252, 198) = gcd(198, 54)$

$198 = 3 \times 54 + 36$ $\quad gcd(198, 54) = gcd(54, 36)$

$54 = 1 \times 36 + 18$ $\quad = gcd(36, 18)$

$36 = 2 \times 18 + 0$ stop $\quad = 18$

Algorithm

- Repeatedly express $a = bq + r$.
- use the key observation that $gcd(a,b) = gcd(b,r)$
- stop when $r = 0$.

See Algorith 1 in 4.3 for a formal expression of Euclid algorithm.

Consider the previous example. Observe that

$$\gcd(252, 198) = 18 = 54 - 1 \times 36 = 54 - 1 \times (198 - 3 \times 54)$$
$$= (-1)\,198 + 4 \times 54 = (-1)\,198 + 4 \times (252 - 198)$$
$$= 4 \times 252 - 5 \times 198$$

Observation: Using the division equations in reverse, we can express $\gcd(a, b) = s \cdot a + t \cdot b$ for some integers $s, t \in \mathbb{Z}$

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

gcd(a,b),
Eclid Algorithm

Repeated squaring
$5^{2024} \bmod 12$

Bezout's theorem
$\exists s,t \in \mathbb{Z}$ $\gcd(a,b) = sa+tb$

FTA: Existence and uniqueness

Bezout's Theorem

If a and b are integers not both zero, then there are $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = sa + tb$.

Proof: Sec 5.2, Exercise 36.

We use Bezout's theorem to prove Euclid's Lemma

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

gcd(a,b),
Eclid Algorithm

Repeated squaring
$5^{2024} \bmod 12$

Bezout's theorem
$\exists s,t \in \mathbb{Z}$ $\gcd(a,b) = sa+tb$

Euclid's Lemma
if $a \mid bc$ and $\gcd(a,b)=1$,
then $a \mid c$

FTA: Existence
and uniqueness

Defn: Two integers a, b are *relatively prime* if $\gcd(a,b) = 1$.

Euclid's Lemma: If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

a and b are relatively prime, i.e., they have no common factor

proof: Assume arbitrary a, b, and c such that $a \mid bc$ and $\gcd(a,b) = 1$. By Bezout's lemma, we can choose s and t s.t. $sa + tb = 1$. Note that $sac + tbc = c$. Since $a \mid sca$ and $a \mid bc$, we have that $a \mid sac + tbc$. Thus, $a \mid c$ as desired. $\square$

Corollary of Euclid's lemma:

If p is a prime and $p \mid a_1 a_2 \cdots a_k$ then $p \mid a_j$ for some a_j.

Proof: Sec 5.1, Exercise 64.

We proceed by induction.

Base Case ($n=1$): Assume arbitrary prime p and integer a_1. By the assumption of the implication $p \mid a_j$ for some a_j, namely $j=1$.

Inductive Step: Assume arbitrary $k \geq 1$. Assume that for any $a_1 \cdots a_k$ if $p \mid a_1 \times \cdots \times a_k$ then $p \mid a_j$ for some $j \in \{1, \ldots, k\}$.

We have to show that for any $b_1, \ldots, b_{k+1}$, if $p \mid b_1 \cdots b_{k+1}$

then $p \mid b_j$ for some $j \in \{1, \dots, k+1\}$

Let us look at $\gcd(p, b_1, \dots, b_k)$. Since p is a prime only $p \mid p$ and $1 \mid p$. Hence, $\gcd(p, b_1 \times \cdots \times b_k)$ is either 1 or p.

- If $\gcd(p, b_1 \times \cdots \times b_k) = 1$, then by Euclid's lemma $p \mid b_{k+1}$, as desired.
- If $\gcd(p, b_1 \times \cdots \times b_k) = p$, then $p \mid b_1 \times \cdots \times b_k$, by the assumption of the inductive step, $p \mid b_j$ for some $j \in \{1, \dots, k\}$ as desired. $\square$

division Alg
$a = dq + r$, $0 \leq r < d$

modular arithmetic
$a \equiv b \pmod{m} \longleftrightarrow m \mid a-b$

Binary, base b representation

gcd(a,b),
Eclid Algorithm

Repeated squaring
$5^{2024} \bmod 12$

Bezout's theorem
$\exists s,t \in \mathbb{Z}$ $\gcd(a,b) = sa+tb$

Euclid's Lemma
if $a \mid bc$ and $\gcd(a,b)=1$,
then $a \mid c$

FTA: Existence
and uniqueness

Now we are ready to finish the uniqueness proof of FTA.

proof of uniqueness: Assume for contradiction that there exists $n>1$ such that $n=p_1p_2\cdots p_k=q_1q_2\cdots q_\ell$ where $p_1\leq p_2\leq\cdots\leq p_k$ and $q_1\leq q_2\leq\cdots\leq q_\ell$ are primes. Assume without loss of generality that $p_i\neq q_j$ for every i and j. Note that $p_1\mid q_1\times\cdots\times q_\ell$. Then by Corrolary of Euclid's lemma, choose $j\in\{1,\dots,\ell\}$ such that $p\mid q_j$. Since p is a prime $q_j=p$, which is a contradiction.