

Foundations of Computer Science

Lecture 10

Number Theory

Division and the Greatest Common Divisor
Fundamental Theorem of Arithmetic
Cryptography and Modular Arithmetic
RSA: Public Key Cryptography



Last Time

- 1 Why sums and recurrences? Running times of programs.
- 2 Tools for summation: constant rule, sum rule, common sums and nested sum rule.
- 3 Comparing functions - asymptotics: Big-Oh, Theta, Little-Oh notation.
 $\log \log(n) < \log^\alpha(n) < n^\epsilon < 2^{\delta n}$
- 4 The method of integration - estimating sums.

$$\sum_{i=1}^n i^k \sim \frac{n^{k+1}}{k+1} \quad \sum_{i=1}^n \frac{1}{i} \sim \ln n \quad \ln n! = \sum_{i=1}^n \ln i \sim n \ln n - n$$

Today: Number Theory

- 1 Division and Greatest Common Divisor (GCD)
 - Euclid's algorithm
 - Bezout's identity
- 2 Fundamental Theorem of Arithmetic
- 3 Modular Arithmetic
 - Cryptography
 - RSA public key cryptography

Number theory Attracts the Best of the Best

“Babies can ask questions which grown-ups can't solve” – P. Erdős

$6 = 1 + 2 + 3$ is *perfect* (equals the sum of its proper divisors).

Is there an odd perfect number?

The Basics

Quotient-Remainder Theorem

For $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, $n = qd + r$. The quotient $q \in \mathbb{Z}$ and remainder $0 \leq r < d$ are *unique*.

e.g. $n = 27, d = 6$: $27 = 4 \cdot 6 + 4 \rightarrow \text{rem}(27, 6) = 4$.

Divisibility. d divides n , $d|n$ if and only if $n = qd$ for some $q \in \mathbb{Z}$. e.g. $6|24$.

Primes. $P = \{2, 3, 5, 7, 11, \dots\} = \{p \mid p \geq 2 \text{ and the only positive divisors of } p \text{ are } 1, p\}$.

Division Facts (Exercise 10.2)

- | | |
|---|--|
| 1 $d 0$. | 4 If $d n$ and $d m$, then $d n+m$. |
| 2 If $d m$ and $d' n$, then $dd' mn$. | 5 If $d n$, then $xd xn$ for $x \in \mathbb{N}$. |
| 3 If $d m$ and $m n$, then $d n$. | 6 If $d m+n$ and $d m$, then $d n$. |

Greatest Common Divisor

Divisors of 30: $\{1, 2, 3, 5, 6, 10, 15, 30\}$. Divisors of 42: $\{1, 2, 3, 6, 7, 14, 21, 42\}$. Common divisors: $\{1, 2, 3, 6\}$.
greatest common divisor (GCD) = 6.

Definition. Greatest Common Divisor, GCD

Let m, n be two integers not both zero. $\text{gcd}(m, n)$ is the largest integer that divides both m and n : $\text{gcd}(m, n)|m$, $\text{gcd}(m, n)|n$ and any other common divisor $d \leq \text{gcd}(m, n)$.

Notice that every common divisor divides the GCD. Also, $\text{gcd}(m, n) = \text{gcd}(n, m)$.

Relatively Prime

If $\text{gcd}(m, n) = 1$, then m, n are relatively prime.

Example: 6 and 35 are not prime but they are relatively prime.

Theorem.

$\text{gcd}(m, n) = \text{gcd}(\text{rem}(n, m), m)$.

Proof. $n = qm + r \rightarrow r = n - qm$. Let $D = \text{gcd}(m, n)$ and $d = \text{gcd}(m, r)$.
 $D|m$ and $D|n \rightarrow D$ divides $r = n - qm$. Hence, $D \leq \text{gcd}(m, r) = d$. (D is a common divisor of m, r)
 $d|m$ and $d|r \rightarrow d$ divides $n = qm + r$. Hence, $d \leq \text{gcd}(m, n) = D$. (d is a common divisor of m, n)
 $D \leq d$ and $D \geq d \rightarrow D = d$, which proves $\text{gcd}(m, n) = \text{gcd}(n, r)$. ■

Euclid's Algorithm

Theorem.

$\text{gcd}(m, n) = \text{gcd}(\text{rem}(n, m), m)$.

$$\begin{aligned} \text{gcd}(42, 108) &= \text{gcd}(24, 42) & 24 &= 108 - 2 \cdot 42 \\ &= \text{gcd}(18, 24) & 18 &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot 42 - 108 \\ &= \text{gcd}(6, 18) & 6 &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot 108 - 5 \cdot 42 \\ &= \text{gcd}(0, 6) & 0 &= 18 - 3 \cdot 6 \\ &= 6 & \text{gcd}(0, n) &= n \end{aligned}$$

Remainders in Euclid's algorithm are integer linear combinations of 42 and 108.

In particular, $\text{gcd}(42, 108) = 6 = 2 \times 108 - 5 \times 42$.

This will be true for $\text{gcd}(m, n)$ in general:

$$\text{gcd}(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Bezout's Identity: A "Formula" for GCD

From Euclid's Algorithm,

$$\text{gcd}(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Can any smaller positive number z be a linear combination of m and n ?

suppose: $z = mx + ny > 0$.

$\text{gcd}(m, n)$ divides RHS $\rightarrow \text{gcd}(m, n)|z$, i.e. $z \geq \text{gcd}(m, n)$ (because $\text{gcd}(m, n)|m$ and $\text{gcd}(m, n)|n$).

Theorem. Bezout's Identity

$\text{gcd}(m, n)$ is the *smallest positive integer linear combination* of m and n :

$$\text{gcd}(m, n) = mx + ny \quad \text{for } x, y \in \mathbb{Z}.$$

Formal Proof. Let ℓ be the smallest positive linear combination of m, n : $\ell = mx + ny$.

- Prove $\ell \geq \text{gcd}(m, n)$ as above.
- Prove $\ell \leq \text{gcd}(m, n)$ by showing ℓ is a common divisor ($\text{rem}(m, \ell) = \text{rem}(n, \ell) = 0$).

There is no "formula" for GCD. But this is close to a "formula".

GCD Facts

- ① $\gcd(m, n) = \gcd(m, \text{rem}(n, m))$. ✓
- ② Every common divisor of m, n divides $\gcd(m, n)$. ✓
- ③ For $k \in \mathbb{N}$, $\gcd(km, kn) = k \cdot \gcd(m, n)$. ✓
- ④ IF $\gcd(l, m) = 1$ AND $\gcd(l, n) = 1$, THEN $\gcd(l, mn) = 1$. ✓
- ⑤ IF $d|mn$ AND $\gcd(d, m) = 1$, THEN $d|n$. ✓

Proof.

- ① $\gcd(m, n) = mx + ny$. Any common divisor divides the RHS and so also the LHS.
(e.g. 1,2,3,6 are common divisors of 30,42 and all divide the GCD 6)
- ② $\gcd(km, kn) = kmx + kny = k(mx + ny)$. The RHS is the smallest possible, so there is no smaller positive linear combination of m, n . That is $\gcd(m, n) = (mx + ny)$.
(e.g. $\gcd(6, 15) = 3 \rightarrow \gcd(12, 30) = 2 \times 3 = 6$)
- ③ $1 = \ell x + my$ and $1 = \ell x' + ny'$. Multiplying,
 $1 = (\ell x + my)(\ell x' + ny') = \ell \cdot (\ell x x' + n x y' + m y x') + m n \cdot (y y')$.
(e.g. $\gcd(15, 4) = 1$ and $\gcd(15, 7) = 1 \rightarrow \gcd(15, 28) = 1$)
- ④ $dx + my = 1 \rightarrow ndx + nmy = n$. Since $d|mn$, d divides the LHS, hence $d|n$, the RHS.
(e.g. $\gcd(4, 15) = 1$ and $4|15 \times 16 \rightarrow 4|16$)

Die Hard: With A Vengeance, John McClane & Zeus Carver Thwart Simon Gruber

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

- 1: Repeatedly fill the 3-gallon jug.
 - 2: Empty the 3-gallon jug into the 5-gallon jug.
 - 3: If ever the 5-gallon jug is full, empty it by discarding the water.
- $(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \xrightarrow{1} (3, 1) \xrightarrow{2} (0, 4) \checkmark$

After the 3-gallon jug is emptied into the 5-gallon jug, the state is $(0, \ell)$, where

$$\ell = 3x - 5y.$$

(the 3-gallon jug has been emptied x times and the 5-gallon jug y times)

(integer linear combination of 3, 5). Since $\gcd(3, 5) = 1$ we can get $\ell = 1$,

$$1 = 3 \cdot 2 - 5 \cdot 1$$

(after emptying the 3-gallon jug 2 times and the 5 gallon jug once, there is 1 gallon)

Do this 4 times and you have 4 gallons (guaranteed). (Actually fewer pours works.)

$$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \quad (\text{repeat 4 times})$$

If the producers of Die Hard had chosen 3 and 6 gallon jugs, there can be no sequel (pew 😊). (Why?)

Fundamental Theorem of Arithmetic Part (ii)

Theorem. Uniqueness of Prime Factorization
Every $n \geq 2$ is *uniquely* (up to reordering) a product of primes.

Euclid's Lemma: For primes p, q_1, \dots, q_ℓ , if $p|q_1q_2 \dots q_\ell$ then p is one of the q_i .
Proof of lemma: If $p|q_\ell$ then $p = q_\ell$. If not, $\gcd(p, q_\ell) = 1$ and $p|q_1 \dots q_{\ell-1}$ by GCD fact (v). Induction on ℓ .

Proof. (FTA) Contradiction. Let n_* be the smallest counter-example, $n_* > 2$ and

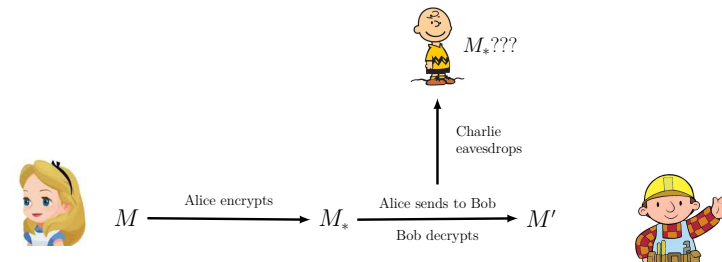
$$\begin{aligned} n_* &= p_1 p_2 \dots p_n \\ &= q_1 q_2 \dots q_k \end{aligned}$$

Since $p_1|n_*$, it means $p_1|q_1q_2 \dots q_k$ and by Euclid's Lemma, $p_1 = q_i$ (w.l.o.g. q_1).

$$\begin{aligned} n_*/p_1 &= p_2 \dots p_n \\ &= q_2 \dots q_k. \end{aligned}$$

That is, n_*/p_1 is a smaller counter-example. **FISHY!**

Cryptography 101: Alice and Bob wish to securely exchange the prime M



Example.
Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)
Alice and Bob know k , Charlie does not.
Bob Decrypts: $M' = M_*/k = M \times k/k = M$. (Hooray, $M' = M$ and Charlie is in the dark.)

Secure as long as Charlie cannot factor M' into k and M . (Factoring is HARD)
One time use. For two *cypher-texts*, $k = \gcd(M_{1*}, M_{2*})$.
To improve, we need modular arithmetic.

Modular Arithmetic

$$a \equiv b \pmod{d} \quad \text{if and only if} \quad d|(a-b), \quad \text{i.e. } a-b = kd \text{ for } k \in \mathbb{Z}$$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$. Then,

$$(a) \ ar \equiv bs \pmod{d}. \quad (b) \ a + r \equiv b + s \pmod{d}. \quad (c) \ a^n \equiv b^n \pmod{d}.$$

| | | |
|--|--|---|
| $\begin{aligned} ar - bs &= (b + kd)(s + \ell d) - bs \\ &= d(ks + b\ell + k\ell d). \end{aligned}$ <p>That is $d ar - bs$.</p> | $\begin{aligned} (a+r) - (b+s) &= (b + kd + s + \ell d) - b - s \\ &= d(k + \ell). \end{aligned}$ <p>That is $d (a+r) - (b+s)$.</p> | <p>Repeated application of (a) Induction.</p> |
|--|--|---|

Addition and multiplication are just like regular arithmetic.

Example. What is the last digit of 3^{2017} ?

$$\begin{aligned} 3^2 &\equiv -1 \pmod{10} \\ \rightarrow (3^2)^{1008} &\equiv (-1)^{1008} \pmod{10} \\ \rightarrow 3 \cdot (3^2)^{1008} &\equiv 3 \cdot (-1)^{1008} \pmod{10} \\ &\equiv 3 \end{aligned}$$

Modular Division is Not Like Regular Arithmetic

$$\begin{aligned} 15 \cdot 8 &\equiv 13 \cdot 8 \pmod{12} & 15 \cdot 8 &\equiv 2 \cdot 8 \pmod{13} & 7 \cdot 8 &\equiv 22 \cdot 8 \pmod{15} \\ 15 &\not\equiv 13 \pmod{12} \quad \times & 15 &\equiv 2 \pmod{13} \quad \checkmark & 7 &\equiv 22 \pmod{15} \quad \checkmark \end{aligned}$$

Modular Division: cancelling a factor from both sides

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

Proof. $d|c(a-b)$. By GCD fact (v), $d|a-b$ because $\gcd(c, d) = 1$. ■

If d is prime, then division with prime modulus is pretty much like regular division.

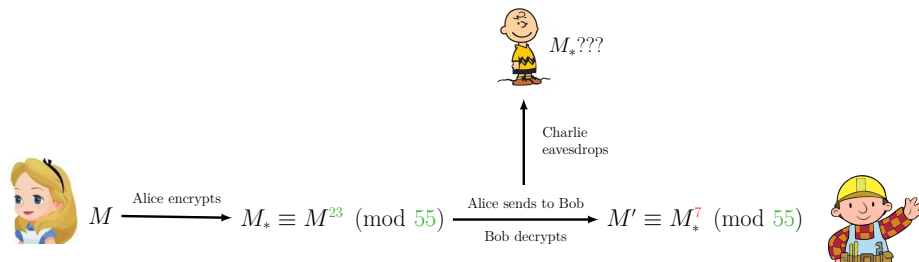
Modular Inverse. Inverses do not exist in \mathbb{N} . Modular inverse may exist.

$$\begin{aligned} 3 \times n &= 1 & n &=? \\ 3 \times n &\equiv 1 \pmod{7} & n &= 5 \end{aligned}$$

RSA Public Key Cryptography Uses Modular Arithmetic

Bob broadcasts to the world the numbers **23, 55**.

(Bob's RSA *public key*).



Examples. Does Bob always decode to the correct message?

| | | | |
|----------|------------------------------|---------------------------|------------|
| $M = 2.$ | $M_* = 8$ | $M' = 2$ | $M' = M$ 😊 |
| | $2^{23} \equiv 8 \pmod{55}$ | $8^7 \equiv 2 \pmod{55}$ | |
| $M = 3.$ | $M_* = 27$ | $M' = 3$ | $M' = M$ 😊 |
| | $3^{23} \equiv 27 \pmod{55}$ | $27^7 \equiv 3 \pmod{55}$ | |

Exercise 10.14. Proof that Bob always decodes to the right message for special **55, 23** and **7**. (How to get them?)

Practical Implementation. Good idea to pad with random bits to make the cypher text random.