CS250: Discrete Math for Computer Science

L5: Divisibility and Modular Arithmetic

Discussion 2: Using the Schröder-Bernstein Theorem

Schröder-Bernstein: $|A| \leq |B| \ \wedge \ |B| \leq |A| \ \rightarrow \ |A| = |B|$

If $\exists f : A \overset{1:1}{\rightarrow} B$ and $\exists g : B \overset{1:1}{\rightarrow} A$ **Then** $\exists h : A \underset{\text{onto}}{\overset{1:1}{\rightarrow}} B$

D2. Use Schröder-Bernstein Thm to show $|R| = |P(\mathbf{N})|$.

1. Construct $f : (0,1) \overset{1:1}{\rightarrow} P(\mathbf{N})$

$r \in (0,1)$ represented in binary number: $r = .b_0 b_1 b_2 b_3 \ldots$.

Note: $\frac{1}{2} = .1 = .0111\ldots = \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$

Solution: If possible, represent r using finitely many non-zero bits!

Each set set $S \subseteq \mathbf{N}$ can be represented as $S : a_0 a_1 a_2 \ldots$ where $a_i = 1$ iff $i \in S$, e.g., Odd $= 010101\ldots$

Finally, let $f(r) = f(.b_0 b_1 b_2 b_3 \ldots) = \left\{ i \in \mathbf{N} \;\middle|\; b_i = 1 \right\}$.

1:1 if $r = .b_0 b_1 b_2 b_3 \ldots \neq s = .c_0 c_1 c_2 c_3 \ldots$ then some $c_i \neq b_i$.
Thus $f(r) \neq f(s)$ because $i \in f(r) \ \Leftrightarrow \ i \notin f(s)$.

2. Construct $g : P(\mathbf{N}) \overset{1:1}{\to} (0,1)$

Each set set $S \subseteq \mathbf{N}$ can be represented as $S : a_0 a_1 a_2 \ldots$ where $a_i = 1$ iff $i \in S$, e.g., Odd $= 010101\ldots$

Note: $\frac{1}{2} = .1 = .0111\ldots = \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$

If we defined g as in f, then **not 1:1** because $S = \{0\}$ and $T = \mathbf{N}^+$ would map to **different representations** of the **same number**.

Solution: For $S = a_0 a_1 a_2 \ldots$ let $g(S) = .a_0 a_1 a_2 \ldots$ **in decimal**

g is **1:1** If $S \neq T$ Then $g(S) \neq g(T)$ because different digits, no 9's. □

Integer Divisibility: definition and examples

For the next few lectures, let the **universe of discourse** be $\mathbf{Z}$, i.e., when we write $\exists x$, $\forall x$, we mean $\exists x \in \mathbf{Z}$, $\forall x \in \mathbf{Z}$.

For $a \neq 0, b \in \mathbf{Z}$, a **divides** b $(a|b)$ iff $\exists d(ad = b)$.

Examples: $3|6$, $2|6$, $4 \nmid 6$

$\exists$-intro proof rule: To prove $\exists x F(x)$ construct t and prove $F(t)$.

let $d_1 = 2$, $2 \in \mathbf{Z}$, $3 \cdot 2 = 6$, thus, $3|6$.

let $d_2 = 3$, $3 \in \mathbf{Z}$, $2 \cdot 3 = 6$, thus, $2|6$.

Suppose $4 \cdot d = 6$, $d = \frac{6}{4} = \frac{3}{2} \notin \mathbf{Z}$, thus, $4 \nmid 6$

Remember the definition: $a|b$ iff $\exists d(ad = b)$

Observation: $\forall x(1|x)$.

$\forall$-intro proof rule: To prove $\forall x F(x)$ let t be an **arbitrary** element of the universe and prove $F(t)$.

Let $t \in \mathbf{Z}$ be **arbitrary**

$1 \cdot t = t$ thus, $1|t$

Since $t \in \mathbf{Z}$ was **arbitrary**, we have shown $\forall x(1|x)$. $\square$

Remember the definition: $a|b$ iff $\exists d(ad = b)$

Proposition: For all $a \neq 0, b, c$,

1. $a|b \ \wedge \ a|c \rightarrow a|(b + c)$
2. $a|b \rightarrow a|(bc)$
3. $a|b \wedge b|c \rightarrow a|c$

$\rightarrow$-intro proof rule: To prove $F \rightarrow G$ **assume** F and **prove** G.

Proof.

1. Suppose $ad_1 = b$, $ad_2 = c$, then $a(d_1 + d_2) = b + c$.
2. Suppose $ad = b$, then $a(dc) = bc$.
3. Suppose $ad_1 = b$, $bd_2 = c$, then $a(d_1 d_2) = c$.

Modular Arithmetic

Fix a **modulus** m, and for any other number a consider the **remainder** when a is divided by m.

Notation: For $m > 1$, $a \bmod m = a \,\%\, m$ is the remainder when a is divided by m. **always:** $0 \leq r < m$

Examples:

$$\begin{aligned}
3 \bmod 10 &= 3 \\
21 \bmod 10 &= 1 \\
128 \bmod 10 &= 8 \\
-7 \bmod 10 &= 3 \\
3 \bmod 2 &= 1 \\
21 \bmod 2 &= 1 \\
128 \bmod 2 &= 0 \\
-7 \bmod 2 &= 1
\end{aligned}$$

Def: a is **congruent** to b mod m $\quad (a \equiv b \pmod{m})$

$$a \equiv b \pmod{m} \quad \text{iff} \quad (a \bmod m) = (b \bmod m) \quad \text{iff} \quad m|(a-b).$$

Examples:

$$\begin{aligned} 3 &\equiv 13 \pmod{10} \\ 3 &\equiv -7 \pmod{10} \\ 128 &\equiv 13 \pmod{5} \\ 128 &\equiv 0 \pmod{2} \end{aligned}$$

Def: a is the **multiplicative inverse** of b mod m iff $(ab \equiv 1 \pmod{m})$

Examples:

$$7 \cdot 3 \equiv 1 \pmod{10}$$
$$5 \cdot 5 \equiv 1 \pmod{8}$$

3 and 7 are multiplicative inverses (mod 10)

5 is its own multiplicative inverse (mod 8)

2 has no multiplicative inverse (mod 4). **Why?**

Casting Out Nines

A trick for checking multiplication that they used to teach in elementary school.

After multiplying two numbers, here's a check that you are right:

Sum the digits and multiply the sums of digits:

$$25 \times 289 = 7225$$

$$7 \times 1 = 7$$

$2 + 5 \rightarrow 7$
$2 + 8 + 9 \rightarrow 19 \rightarrow 10 \rightarrow 1$
$7 + 2 + 2 + 5 \rightarrow 16 \rightarrow 7$

Why does this work?

Because casting out by nines, is the same as reducing mod 9.

$10 \equiv 1 \pmod 9$

$10^2 \equiv 1 \pmod 9 \quad 10^3 \equiv 1 \pmod 9 \cdots$

$$\begin{aligned}
7225 &= 7 \cdot 10^3 + 2 \cdot 10^2 + 2 \cdot 10^1 + 5 \cdot 1 \\
&\equiv 7 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 5 \cdot 1 && \pmod 9 \\
&\equiv 16 && \pmod 9 \\
&\equiv 1 \cdot 10 + 6 \cdot 1 && \pmod 9 \\
&\equiv 1 \cdot 1 + 6 \cdot 1 && \pmod 9 \\
&\equiv 7 && \pmod 9
\end{aligned}$$

IF $a \cdot b = c$ THEN $a \cdot b \equiv c \pmod 9$.

Changing Bases

Base 10: $215 = 2 \cdot 10^2 + 1 \cdot 10 + 5$

Changing from base 10 to base 8:

$$\begin{aligned} 215 &= 26 \cdot 8 + 7 \\ 26 &= 3 \cdot 8 + 2 \\ 3 &= 0 \cdot 8 + 3 \end{aligned}$$

Thus,

$$215 = (327)_8 = 3 \cdot 64 + 2 \cdot 8 + 7 = 192 + 16 + 7 = 215$$

Changing from base 10 to base 2: $215 = (327)_8$

$$
\begin{aligned}
215 &= 107 \cdot 2 + 1 \\
107 &= 53 \cdot 2 + 1 \\
53 &= 26 \cdot 2 + 1 \\
26 &= 13 \cdot 2 + 0 \\
13 &= 6 \cdot 2 + 1 \\
6 &= 3 \cdot 2 + 0 \\
3 &= 1 \cdot 2 + 1 \\
1 &= 0 \cdot 2 + 1
\end{aligned}
$$

$$215 = (11\,010\,111)_2 = (327)_8$$

How long does this take? **It's Fast: one division per digit.**

Exponentiating mod m with huge exponents

Say we want to compute:

$$a^e \pmod{m}$$

but $a, e,$ and m **have a thousand bits each!**

It's not feasible to raise a to the e power because that would be too large: about a million-bit number.

Much better to iteratively **square** a and then **reduce mod** m

How many times?

The number of bits of the exponent $= \log e$

Example: $234^{215} \pmod{1000}$ $\quad 215 = (11010111)_2$

$$
\begin{aligned}
234^1 &\equiv 234 \equiv 234 \equiv 234 \pmod{1000} \\
234^2 &\equiv 234^2 \equiv 54756 \equiv 756 \pmod{1000} \\
234^4 &\equiv 756^2 \equiv 571536 \equiv 536 \pmod{1000} \\
234^8 &\equiv 536^2 \equiv 287296 \equiv 296 \pmod{1000} \\
234^{16} &\equiv 296^2 \equiv 87616 \equiv 616 \pmod{1000} \\
234^{32} &\equiv 616^2 \equiv 379456 \equiv 456 \pmod{1000} \\
234^{64} &\equiv 456^2 \equiv 207936 \equiv 936 \pmod{1000} \\
234^{128} &\equiv 936^2 \equiv 876096 \equiv 96 \pmod{1000}
\end{aligned}
$$

$$
\begin{aligned}
234^{215} &\equiv 234 \cdot 234^2 \cdot 234^4 \cdot 234^{16} \cdot 234^{64} \cdot 234^{128} \pmod{1000} \\
&\equiv 234 \cdot 756 \cdot 536 \cdot 616 \cdot 936 \cdot 96 \pmod{1000} \\
&\equiv 24 \pmod{1000}
\end{aligned}
$$

iClicker: what is $7^{10} \pmod{11}$?

$$10 = (1\,0\,1\,0)_2$$

$$\begin{aligned}
7^1 &\equiv 7 \equiv 7 \equiv 7 \pmod{11} \\
7^2 &\equiv 7^2 \equiv 49 \equiv 5 \pmod{11} \\
7^4 &\equiv 5^2 \equiv 25 \equiv 3 \pmod{11} \\
7^8 &\equiv 3^2 \equiv 9 \equiv 9 \pmod{11}
\end{aligned}$$

A: 0

B: 7

C: 10

D: 1

E: 4

Greatest Common Divisors, GCD

If $d|a$ and $d|b$ then d is a **common divisor** of a and b.

1, 2, 3, and 6 are common divisors of $12, 18$.

1 is a common divisor of every pair of integers a, b.

The **greatest common divisor** of a, b is denoted $\gcd(a, b)$.

$$\gcd(12, 18) = 6$$

$$\gcd(5, 11) = 1$$

$$\gcd(17, 34) = 17$$

$$\gcd(30, 100) =$$ A 1 B 2 C 5 **D** 10 E 15

$$\gcd(98, 105) =$$ A 1 B 2 C 3 D 5 **E** 7

How do we efficiently compute $\gcd(a, b)$?

Easy if we know the prime factors of a and b:

$12 = 2^2 \cdot 3^1$ $\quad$ $18 = 2^1 \cdot 3^2$ $\quad$ $\gcd(12, 18) = 2^1 \cdot 3^1$

$5 = 5^1 \cdot 11^0$ $\quad$ $11 = 5^0 \cdot 11^1$ $\quad$ $\gcd(5, 11) = 5^0 \cdot 11^0$

$17 = 2^0 \cdot 17^1$ $\quad$ $34 = 2^1 \cdot 17^1$ $\quad$ $\gcd(17, 34) = 2^0 \cdot 17^1$

$30 = 2^1 \cdot 3^1 \cdot 5^1$ $\quad$ $100 = 2^2 \cdot 3^0 \cdot 5^2$ $\quad$ $\gcd(30, 100) = 2^1 \cdot 3^0 \cdot 5^1$

$98 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^2$ $\quad$ $105 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1$ $\quad$ $\gcd(98, 105) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1$

Prop: If $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}$
for primes $p_1 < p_2 < \cdots < p_k$,

Then $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$

But, factoring integers is computationally difficult

To factor a thousand-bit integer, a,

we would try all divisors up to $\sqrt{a}$

but that we would be about 2^{500} divisors!

This is **exponential time** in terms of the size of the input, so it is **not feasible**.

Next time, we will see how over 2300 years ago, Euclid gave a very efficient algorithm to compute $\gcd(a, b)$**, without factoring.**

This was in Euclid's Geometry text. He was thinking about line segments and wanted to be able to compute the length d **of the longest line segment that evenly divided two given line segments,** a **and** b**.**