Tut 7 & Review

Jingyu Li

Definition. $a \equiv b \pmod{n}$ iff $n \mid (a - b)$.

Claim: $a \equiv b \pmod{n} \Leftrightarrow a \bmod n = b \bmod n$

Theorem. If $\gcd(k,n)=1$, then have k' such that

$$k \cdot k' \equiv 1 \pmod{n},$$

where k' is an *inverse* of $k \pmod{n}$.

Theorem. Let p be a prime and $\gcd(k,p) = 1$. Then

$$k^{p-1} \equiv 1 \pmod{p}.$$

Theorem. p is a prime if and only if

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

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

Set $x = 5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c$

Then the first (second, third) term is determined by the first (second, third) equation.

Now we just need to solve the following equations separately.

$$35a \equiv 2 \pmod 3,\quad 21b \equiv 4 \pmod 5,\quad 15c \equiv 6 \pmod 7.$$

$$\Rightarrow\quad 2a \equiv 2 \pmod 3,\quad b \equiv 4 \pmod 5,\quad c \equiv 6 \pmod 7.$$

$$\Rightarrow\quad a \equiv 1 \pmod 3,\quad b \equiv 4 \pmod 5,\quad c \equiv 6 \pmod 7.$$

Then $x = 35a + 21b + 15c \equiv 35 \cdot 1 + 21 \cdot 4 + 15 \cdot 6 \pmod{3 \cdot 5 \cdot 7} \equiv 209 \pmod{105}$.

Since Han Xin (韓信) knew that $1000 \le x \le 1100$, he concluded that $x = 1049$.

faster method.

$$x = 3a+2 \quad (a \in \mathbb{Z})$$

$$3a+2 \equiv 4 \pmod 5$$

$$\Rightarrow \quad 3a \equiv 2 \pmod 5$$

$$2 \cdot 3a \equiv 2 \cdot 2 \pmod 5$$

$$a \equiv 4 \pmod 5$$

$$a = 5b+4 \quad (b \in \mathbb{Z})$$

$$x = 3a+2 = 3(5b+4)+2 = \cdots$$

Question

Find the smallest positive three consecutive integers such that they are divisible by 4,9,25 respectively.

Assume the largest int a. $(a-1)$ $(a-2)$

$$\begin{cases} a \equiv 0 \pmod{25} \\ a \equiv 1 \pmod{9} \\ a \equiv 2 \pmod{4} \end{cases}$$

$a = 25b \ (b \in \mathbb{Z})$

$25b \equiv 1 \pmod{9} \Rightarrow 7b \equiv 1 \pmod{9}$

$7 \cdot 4b \equiv 4 \pmod{9} \Rightarrow b \equiv 4 \pmod{9}$

$b = 4 + 9c \ (c \in \mathbb{Z})$

$a = 25(4+9c) = 100 + 225c$

$\cancel{100} + 225c \equiv 2 \pmod{4}$

$c \equiv 2 \pmod{4}$

$c = 4d + 2 \ (d \in \mathbb{Z})$

$a = 100 + 225(4d+2)$

$= 900d + 550 \ (d \in \mathbb{Z})$

$a \equiv 550 \pmod{900}$

$a = 550$ 548、549、550

$$\begin{cases} a \equiv 0 \pmod{25} \\ a \equiv 1 \pmod{9} \\ a \equiv 2 \pmod{4} \end{cases}$$

$$a = 25 \times 9\, x + 25 \times 4\, y + 9 \times 4\, z$$
$$= 225x + 100y + 36z$$

(1) $36z \equiv 0 \pmod{25}$

$z \equiv 0 \pmod{25}$

(2) $225x \equiv 2 \pmod{4}$

$x \equiv 2 \pmod{4}$

(3) $100y \equiv 1 \pmod{9}$

$y \equiv 1 \pmod{9}$

$$a = (225 \times 2 + 25 \times 4 \times 1 + 9 \times 4 \times 0) + (4 \times 9 \times 25)n$$
$$= 550 + 900n$$ 550

Prove that a number is divisible by 11 if and only if the sum of its digits, where every other one is negated, is divisible by 11.

Example:

$3-7+2-7+3-7+6-1+2-6+1=-11$

$37273761261=11\times 3388523751$

121

Assume $n=\overline{d_k d_{k-1} d_{k-2}\cdots d_1 d_0}$

$= d_k\cdot 10^k + d_{k-1}\cdot 10^{k-1} + \cdots + d_1\cdot 10^1 + d_0$

$10\equiv -1 \pmod{11}$ $\qquad$ $n \bmod 11$

$10^k\equiv(-1)^k \pmod{11}$ $\qquad$ $= d_k\cdot(-1)^k + d_{k-1}\cdot(-1)^{k-1} + \cdots d_1\cdot(-1) + d_0$

$(\;-1 \quad 1 \;-1 \quad 1 \;-)$

Question

Let $a \in Z^+$, $b \in Z^+$ be such that $\gcd(a,b) = 1$. Prove that there exists $n \in Z^+$ such that $a^n \equiv 1 \pmod{b}$.

$\gcd = spc$ $\quad sa+tb=1 \quad sa-1=-tb$

$\exists s.t \in Z, \quad \underline{sa} \equiv 1 \pmod{b}$

Lemma. If $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$ then $ab \equiv cd \pmod{n}$.

If $a \equiv c \pmod{n}$, and if $m \geq 0$ is an integer, then

(i) $a^m \equiv c^m \pmod{n}$,

At most b results for $(s^i \bmod b)$

$\exists k.j \in Z^+, \quad s^k \equiv s^j \pmod{b}$

$(k>j)$

$s^j \cdot s^{k-j} \equiv s^j \pmod{b}$

$s^{k-j} \equiv 1 \pmod{b}$

$\gcd(s^j, b) = 1$

$s^k = s^j + bm$

$s^j(s^{k-j}-1) = bm$

pick $n = k - j$ $\quad (s^n \equiv 1^n \pmod b)$

$b \mid s^{k-j} - 1$

$s^{k-j} \equiv 1 \pmod b$

$a^n \equiv a^n \cdot 1^n \equiv a^n \cdot s^n \pmod b$

$(sa)^n \equiv 1 \pmod b$

$a^n \equiv 1 \pmod b$

idea

$(s^n a^n \equiv 1 \pmod b)$

$\Rightarrow s^n \equiv 1 \pmod b$

Question

Let $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}^+$ be such that $\gcd(a,b) = 1$. Prove that there exists $n \in \mathbb{Z}^+$ such that $a^n \equiv 1 \pmod b$.

There are only b resnlts for $(a^i \bmod b)$ $(i \in \mathbb{Z}^+)$.

$\exists k, j \in \mathbb{Z}^+, k > j$:

$a^k \equiv a^j \pmod b$

$a^j \cdot a^{k-j} \equiv a^j \pmod b$ $\quad (\gcd(a^j, b) = 1)$

$a^{k-j} \equiv 1 \pmod b$

$n = k - j$

What we have learned…

roll

got

- 1. Logic and Set
- 2. Proof I (basic, Invariant method, WOP)
- 3. Proof II (Mathematical induction)
- 4. Recursion
- 5. Greatest common divisors
- 6. Modular arithmetic (CRT)

lec. (tut. FQ. asg)

real problems

summarize

1. Logic and Set

$$
\begin{array}{ll}
 & (p \vee q) \rightarrow \neg r \\
\text{(i)} & p \rightarrow \neg q \\
 & \neg q \rightarrow p \\
\hline
\therefore & \neg r
\end{array}
$$

valid / invalid

T → F

2. (*18 points*) Suppose that you are given two "**NOT**"s, two "**AND**"s, and two "**OR**"s of the following electronic components:

<table>
<tr><th>Type of Gate</th><th>Symbolic Representation</th><th>Action</th></tr>
<tr><td>NOT</td><td>P NOT R</td><td><table><tr><th>Input</th><th>Output</th></tr><tr><th>P</th><th>R</th></tr><tr><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td></tr></table></td></tr>
<tr><td>AND</td><td>P Q AND R</td><td><table><tr><th colspan="2">Input</th><th>Output</th></tr><tr><th>P</th><th>Q</th><th>R</th></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table></td></tr>
<tr><td>OR</td><td>P Q OR R</td><td><table><tr><th colspan="2">Input</th><th>Output</th></tr><tr><th>P</th><th>Q</th><th>R</th></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table></td></tr>
</table>

P	Q	R	output
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	1

logical formula

T

F

2. Proof I (basic, Invariant method, WOP)

contradiction

2. (*12 points*) For all integers $n \geq 4$, use **Well Ordering Principle** to prove that

$$n^2 \leq 2^n$$

$S = \{n \in \mathbb{N} \mid \text{satisfy reverse}\}$

$S = \{n \mid n^2 > 2^n\}$

smallest $n \to n_0$

$n_0^2 > 2^{n_0} \to (n_0-2)^2 > \left(\frac{n_0}{2}\right)^2 = \frac{n_0^2}{4} > 2^{n_0-2}$ smaller n_0

$(n_0-2) \in S$ contradiction

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

Parity of S = (number of disorder pairs + i) mod 2

奇偶性，染色法

3. Proof II (Mathematical induction)

6. (*18 points*) A confectionery company is designing an assorted pack of confectionery consisting of chocolate (15g/bag), marshmallow (6g/bag) and toffee (10g/bag). Show that for any pack with an integer weight at least 61g (i.e., 61g, 62g, 63g, etc), there is always a way to mix these three kinds of confectionery so that the pack contains some (≥ 1 bag) of each confectionery.

$P(n)$ → basic case → inductive step

normal / strong

4. Recursion

→ lec slides

3. (*19 points*) Consider the set of all strings of a's, b's and c's. Let r_n be the number of strings of a's, b's and c's of length n that do not contain the patterns aa and ab. ($n \in \mathbb{Z}^+$)

(a) Find the values of r_1, r_2, r_3 by enumerating the strings. **[6 marks]**

(b) Find the recurrence relation for $\{r_n\}$. **[5 marks]**

(c) Find the closed form for r_n. **[8 marks]**

$$a_n = 3a_{n-1} - 2a_{n-2}$$

$$x^2 = 3x - 2$$

$$a_n = C \cdot x_1^n + D \cdot x_2^n$$

5. Greatest common divisors

1. (*11 points*) Find $\gcd(2019! + 1, 2020! + 1)$.

① $\gcd(a.b) = \gcd(b, r)$ Euclid

② $\gcd = spc$

proof: $\gcd(a.b) = 1$

$a|n$、$b|n \Rightarrow ab|n$

6. Modular arithmetic (CRT)

4. (*24 points*) Find the smallest positive integer x satisfying the following:

$$\begin{cases} 95x \equiv 5 \pmod{40} \\ 21x \equiv -9 \pmod{60} \\ 2x \equiv 152 \pmod{75} \end{cases}$$

faster / CRT