Number Theory

Modular arithmetic and GCD

Misha Lavrov

ARML Practice 9/22/2013

Modular arithmetic

Definition

If a, b, m are integers, $m > 0$, we say a and b are equivalent mod m, written $a \equiv b \pmod{m}$, if $a - b$ is a multiple of m.

- $3 \equiv 13 \equiv 333 \equiv 2013 \equiv -7 \equiv -57 \pmod{10}$.
- $1 \equiv 5 \equiv 199 \equiv 2013 \pmod{2}$ and
  $0 \equiv 2 \equiv 8 \equiv 200 \equiv -1444 \pmod{2}$.
- $5 \equiv 12 \equiv 7005 \pmod{7}$.
- $\cdots \equiv -2 \equiv -1 \equiv 0 \equiv 1 \equiv 2 \equiv 3 \equiv \cdots \pmod{1}$.

Modular arithmetic

Definition

If a, b, m are integers, $m > 0$, we say a and b are equivalent mod m, written $a \equiv b \pmod{m}$, if $a - b$ is a multiple of m.

- $3 \equiv 13 \equiv 333 \equiv 2013 \equiv -7 \equiv -57 \pmod{10}$.
- $1 \equiv 5 \equiv 199 \equiv 2013 \pmod{2}$ and
  $0 \equiv 2 \equiv 8 \equiv 200 \equiv -1444 \pmod{2}$.
- $5 \equiv 12 \equiv 7005 \pmod{7}$.
- $\cdots \equiv -2 \equiv -1 \equiv 0 \equiv 1 \equiv 2 \equiv 3 \equiv \cdots \pmod{1}$.
- We also write $a \bmod m$ for the remainder when a is divided by m:

$$b = a \bmod m \quad \Leftrightarrow \quad \begin{cases} 0 \leq b \leq m-1, \\ a \equiv b \pmod{m}. \end{cases}$$

Modular arithmetic
Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$.
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.

Modular arithmetic
Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$. **TRUE**
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$.
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.

Modular arithmetic
Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$. **TRUE**
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. **TRUE**
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$.
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.

Modular arithmetic
Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$. **TRUE**
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. **TRUE**
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$. **FALSE**
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$.
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.

Modular arithmetic

Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$. **TRUE**
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. **TRUE**
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$. **FALSE**
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$. **FALSE**
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$.

Modular arithmetic
Warmup

Reminder: $a \equiv b \pmod{m}$ means $a - b$ is divisible by m.

True or false?

- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$. **TRUE**
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. **TRUE**
- If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$. **FALSE**
- If $ab \equiv 0 \ (m)$, then $a \equiv 0 \ (m)$ or $b \equiv 0 \ (m)$. **FALSE**
- If $ac \equiv bc \pmod{mc}$, then $a \equiv b \pmod{m}$. **TRUE**

Also, both of the false things are **TRUE** if m is prime!

(provided $c \not\equiv 0 \pmod{m}$)

Divisibility rules

1. Suppose x has digits a, b, c, d: that is,

$$x = 1000a + 100b + 10c + d.$$

What is $x \bmod 9$?

Divisibility rules

1. Suppose x has digits a, b, c, d: that is,

$$x = 1000a + 100b + 10c + d.$$

   What is $x \bmod 9$?

   We have $10 = 9 + 1 \equiv 1 \pmod 9$, $100 = 99 + 1 \equiv 1 \pmod 9$, $1000 = 999 + 1 \equiv 1 \pmod 9$, etc. So

$$x \equiv a + b + c + d \pmod 9.$$

2. What is $x \bmod 11$? What about $x \bmod 5$ or $x \bmod 8$?

Divisibility rules

Competition problems

Problem (2003 AIME II, Problem 2.)

Find the greatest integer multiple of 8, no two of whose digits are the same.

Problem (2009 PUMaC Number Theory, Problem A1.)

If $17! = 355687ab8096000$, where a and b are two missing digits, find a and b.

Problem (2004 AIME II, Problem 10.)

Let S be the set of integers between 1 and 2^{40} that contain two 1's when written in base 2. What is the probability that a random integer from S is divisible by 9?

Divisibility rules

Competition problems – solutions to #1 and #2

1. We start from something like 9876543210 and start twiddling digits to make it divisible by 8 (only the last 3 matter). 210 is not divisible by 8, but 120 is, so the answer is 9876543120.
2. We know 17! is divisible both by 9 and by 11, so:

$$\begin{cases} 3+5+5+6+8+7+a+b+8+0+9+6+0+0+0 \\ \qquad \equiv a+b+3 \equiv 0 \pmod 9, \\ 3-5+5-6+8-7+a-b+8-0+9-6+0-0+0 \\ \qquad \equiv a-b-2 \equiv 0 \pmod{11}. \end{cases}$$

The only pair (a, b) that satisfies both conditions is $a = 4,\ b = 2$.

Divisibility rules

Competition problems – solution to #3

We need to make up a rule for divisibility by 9 in base 2. We have

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv -1,\ 2^4 \equiv -2,\ 2^5 \equiv -4,\ 2^6 \equiv 1, \ldots$$

This is kind of terrible for a generic number, but if only two digits of the number are ones, we know that to get 0 mod 9 we need to match up a 1 with a -1, a 2 with a -2, or a 4 with a -4.

Among $\{2^0, \ldots, 2^{39}\}$ there are seven each of $1, 2, 4, -1$ and six each of $-2, -4$. So there are $7 \times 7 + 7 \times 6 + 7 \times 6 = 133$ good pairs out of a total of $\binom{40}{2} = 780$, and the probability is

$$\frac{133}{780}.$$

GCD (Greatest Common Divisor)

Definition

Given two integers $m, n \geq 0$, the GCD[a] of m and n is the largest integer that divides both m and n.

[a] HCF, if you're British

GCD (Greatest Common Divisor)

Definition

Given two integers $m, n \geq 0$, the GCD[a] of m and n is the largest integer that divides both m and n.

[a] HCF, if you're British

$$\begin{aligned} \text{Divisors}(m, n) &:= \{\text{all positive numbers that divide both } m \text{ and } n\} \\ \text{Sums}(m, n) &:= \{\text{all positive numbers of the form } a \cdot m + b \cdot n\} \end{aligned}$$

Fact: $\gcd(m, n)$ is the largest number in $\text{Divisors}(m, n)$, the smallest number in $\text{Sums}(m, n)$, and the only number in both.

The Euclidean algorithm for computing GCD systematically finds smaller and smaller numbers in $\text{Sums}(m, n)$ until it finds one that is also in $\text{Divisors}(m, n)$.

GCD
Problems

1. Compute $\gcd(\underbrace{111\cdots 11}_{300}, \underbrace{111\cdots 11}_{500})$.
2. We define the Fibonacci numbers by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ (they begin 0, 1, 1, 2, 3, 5, ...)
   - Compute $\gcd(F_{100}, F_{99})$ (don't try to compute F_{100} or F_{99})
   - Compute $\gcd(F_{100}, F_{96})$.
3. When does the equation $ax \equiv b \pmod{m}$ have a solution x? (Give a condition that a, b, and m have to satisfy.)

GCD

Solutions

1. If instead of 300 and 500 1's we had 3 and 5, then $\gcd(111, 11111) = \gcd(111, 11111 - 11100) = \gcd(111, 11) = \gcd(111 - 110, 11) = \gcd(1, 11) = 1.$

   If we replace each digit above with 100 copies of that digit, everything is true, so

$$\gcd(\underbrace{111\cdots11}_{300}, \underbrace{111\cdots11}_{500}) = \underbrace{111\cdots11}_{100}.$$

GCD

Solutions

1. If instead of 300 and 500 1's we had 3 and 5, then $\gcd(111, 11111) = \gcd(111, 11111 - 11100) = \gcd(111, 11) = \gcd(111 - 110, 11) = \gcd(1, 11) = 1.$

   If we replace each digit above with 100 copies of that digit, everything is true, so

$$\gcd(\underbrace{111\cdots11}_{300}, \underbrace{111\cdots11}_{500}) = \underbrace{111\cdots11}_{100}.$$

2. $\gcd(F_{100}, F_{99}) = \gcd(F_{100} - F_{99}, F_{99}) = \gcd(F_{98}, F_{99})$ and we can repeat this process to get down to $\gcd(F_0, F_1) = \gcd(0, 1) = 1.$

GCD

Solutions

2. We have

$$F_{100} = F_{99} + F_{98} = 2F_{98} + F_{97} = \cdots = 21F_{93} + 13F_{92}$$
$$F_{96} = F_{95} + F_{94} = 2F_{94} + F_{93} = 3F_{93} + 2F_{92}.$$

So $7F_{96} - F_{100} = (21F_{93} + 14F_{92}) - (21F_{93} + 13F_{92}) = F_{92}$, and $\gcd(F_{100}, F_{96}) = \gcd(F_{96}, F_{92})$. We can repeat this to get down to $\gcd(F_0, F_4) = \gcd(0, 3) = 3$.

GCD

Solutions

2. We have

$$F_{100} = F_{99} + F_{98} = 2F_{98} + F_{97} = \cdots = 21F_{93} + 13F_{92}$$
$$F_{96} = F_{95} + F_{94} = 2F_{94} + F_{93} = 3F_{93} + 2F_{92}.$$

So $7F_{96} - F_{100} = (21F_{93} + 14F_{92}) - (21F_{93} + 13F_{92}) = F_{92}$, and $\gcd(F_{100}, F_{96}) = \gcd(F_{96}, F_{92})$. We can repeat this to get down to $\gcd(F_0, F_4) = \gcd(0, 3) = 3$.

3. If $ax \equiv b \pmod{m}$, that means $ax - b$ is divisible by m, so there is some y such that $ax - b = my$, or $ax - my = b$. This is just saying b is in $\mathrm{Sums}(a, m)$, which happens when b is divisible by $\gcd(a, m)$.