Dr. Z.'s Number Theory Lecture 9 Handout: Modular Arithmetics

By Doron Zeilberger

Version of Oct. 3, 2013 (thanks to Josefina Mansour, who corrected two typos, or rather arithematical errors that I committed by doing 'mental math'). She gets a prize of one dollar.

If it now eleven O'clock (at night), what time is it going to be two hours later? Not thirteen O'clock, but rather one O'clock.

Def.: $a \pmod{b}$ is the remainder obtained by dividing a by b.

Problem 9.1: Find

i. $11 \pmod{5}$ **ii.** $101 \pmod{27}$ **iii.** $1001 \pmod{91}$

Solution of 9.1

i. $11 = 2 \cdot 5 + 1$ (the quotient, 2, is irrelevant!), the remainder is 1, so $11 \pmod{5} = 1$

ii. $101 = 3 \cdot 27 + 20$ (the quotient 3 is irrelevant!), the remainder is 20, so $101 \pmod{27} = 20$

iii. $1001 = 11 \cdot 91 + 0$ (the quotient 11 is irrelevant!), the remainder is 0, so $1001 \pmod{91} = 0$.

Def.: If $a \pmod{c} = b \pmod{c}$ then we write $a \equiv b \pmod{c}$, and say that a and b are **congruent modulo c**. Of course this happens whenever $(a - b)$ is divisible by c.

Problem 9.2: True or False?

i. $5 \equiv 70 \pmod{13}$ **ii.** $11 \equiv 101 \pmod{15}$

Sol. to 9.2: **i.** $70 - 5 = 65$ is divisible by 13, so **true**. **i.** $101 - 11 = 90$ is divisible by 15, so **true**.

How to add modulo m

To find $a + b \pmod{m}$.

Step 1: Find $a \pmod{m}$ and $b \pmod{m}$

Step 2: Add them up

Step 3: Take the remainder upon dividing by m.

Note: If you first add-up a and b, and only take the remainder at the end, you would get the correct answer (if you didn't make a mistake), but it would take longer.

Probelm 9.3: Find $1001 + 9001 \pmod{1000}$.

Sol. to 9.3: $1001 \pmod{1000} = 1$, $9001 \pmod{1000} = 1$, so the answer is $1+1 \pmod{1000} = 2 \pmod{1000} = 2$.

Ans. to 9.3: $2 \pmod{1000}$.

Probelm 9.4: Find $1901 + 9901 \pmod{1000}$.

Sol. to 9.4: $1901 \pmod{1000} = 901$, $9901 \pmod{1000} = 901$, so the answer is $901 + 901 \pmod{1000} = 1802 \pmod{1000} = 802$.

Ans. to 9.4: $802 \pmod{1000}$.

How to multiply modulo m

To find $a \cdot b \pmod{m}$.

Step 1: Find $a \pmod{m}$ and $b \pmod{m}$

Step 2: Multiply them up

Step 3: Take the remainder upon dividing by m.

Note: If you first multiply a and b, and only take the remainder at the end, you would get the correct answer (if you didn't make a mistake), but it would take **much** longer.

Probelm 9.5: Find $1901 \cdot 9901 \pmod{1000}$.

Sol. to 9.5: $1901 \pmod{1000} = 901$, $9901 \pmod{1000} = 901$, so the answer is $901 \cdot 901 \pmod{1000} = 81181 \pmod{1000} = 181$.

Ans. to 9.5: $181 \pmod{1000}$.

How to raise to a power modulo m (Slow way)

To find $a^n \pmod{m}$.

Find, in turn $a, a^2, a^3, \quad, ..., a^n$ but *each time*, take it modulo m.

Note: If you first compute a^n and only take the remainder of division by m at the very end, you would get the correct answer (if you didn't make a mistake), but it would take you **much** longer.

Probelm 9.6: Find $10^{10} \pmod{13}$ using the slow way.

Sol. to 9.6:

$10^2 \pmod{13} = 100 \pmod{13} = 9 \pmod{13}$

$10^3 \pmod{13} = 90 \pmod{13} = 12 \pmod{13}$

$10^4 \pmod{13} = 120 \pmod{13} = 3 \pmod{13}$

$10^5 \pmod{13} = 30 \pmod{13} = 4 \pmod{13}$

$10^6 \pmod{13} = 40 \pmod{13} = 1 \pmod{13}$

$10^7 \pmod{13} = 10 \pmod{13} = 10 \pmod{13}$

$10^8 \pmod{13} = 100 \pmod{13} = 9 \pmod{13}$

$10^9 \pmod{13} = 90 \pmod{13} = 12 \pmod{13}$

$10^{10} \pmod{13} = 120 \pmod{13} = 3 \pmod{13}$

Ans. to 9.5: $3 \pmod{13}$.

How to raise to a power modulo m (Fast way)

To find $a^n \pmod{m}$.

If n is even, first find $b := a^{n/2} \pmod{m}$, and then compute $b^2 \pmod{m}$.

If n is odd, first find $b := a^{n-1} \pmod{m}$, and then compute $a \cdot b \pmod{m}$.

Probelm 9.7: Find $10^{10} \pmod{13}$ using the fast way.

Solution to Problem 9.7:

Downhill journey

Since the power (exponent), $n = 10$, is even, we must first find $10^5 \pmod{13}$, and then square it, modulo 13.

Since 5 is odd, we must first find $10^4 \pmod{13}$, and then multiply it by 10, modulo 13.

Since 4 is even, we must first find $10^2 \pmod{13}$, and then square it, modulo 13.

Since 2 is even, we must first find $10^1 \pmod{13}$, and then square it, modulo 13.

Back journey (uphill)

$10^1 \pmod{13} = 10,$

$10^2 \pmod{13} = 100 \pmod{13} = 9.$

$10^4 \pmod{13} = 9^2 \pmod{13} = 81 \pmod{13} = 3 \pmod{13}$

$10^5 \pmod{13} = 3 \cdot 10 \pmod{13} = 30 \pmod{13} = 4 \pmod{13}$

$10^{10} \pmod{13} = 4^2 \pmod{13} = 16 \pmod{13} = 3 \pmod{13}$

Ans. to 9.7: $3 \pmod{13}$

Another Fast Way: Write n in binary

$$n = \sum_{i=1}^{k} 2^{c_i}$$

where $0 \le c_1 < c_2 < \ldots < c_k$ are the powers of 2 that show up (the places where there are 1's in the binary expansion of n). Let $a_k = K$.

Then prepare a table of $a, a^2, a^4, a^8, \ldots, a^{2^K}$ by repeated squaring, and at the end do

$$a^n = \prod_{i=1}^{k} a^{c_i} \quad .$$

Probelm 9.8: Find $10^{10} \pmod{13}$ using the other fast way.

Sol. to 9.8: $10 = 2^3 + 2^1$.

$10^2 \pmod{13} = 9$

$10^4 \pmod{13} = 9^2 \pmod{13} = 3 \pmod{13}$

$10^8 \pmod{13} = 3^2 \pmod{13} = 9 \pmod{13}$

Finally

$$10^{10} \pmod{13} = (10^8 \pmod{13}) \cdot (10^2 \pmod{13}) = 9 \cdot 9 \pmod{13} = 3 \pmod{13} \quad .$$

Ans. to 9.8: $3 \pmod{13}$