Arithmetic with congruences

Modular Arithmetic and Congruences

Reading

- Section 7.2

Practice Problems

7.2 1, 3, 6, 8, 9, 10, 22, 26
Challenge 7.2 (Optional) 27, 32, 33

Notes

One of the most powerful facts about congruence relations is that they respect arithmetic operations:

> If $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then:
>
> $$a + c \equiv b + d \bmod n$$
>
> $$ac \equiv bd \bmod n$$
>
> $$a^k \equiv b^k \bmod n$$
>
> for all $k \in \mathbb{Z}$.

This has many far-reaching consequences, that we will examine in due course.

The proof of these two statements is fairly straighforward:

- If $n|(b-a)$ and $n|(d-c)$, then it also is the case that $n|(b-a+d-c) = b+d-(a+c)$.
- For the second assertion:
  - If $n|(b-a)$ then it also divides $db-da$.
  - If $n|(d-c)$ then it also divides $ad-ac$.
  - Therefore it divides $db-da+ad-ac = bd-ac$.
- The third assertion follows by induction and using the second assertion.

As a simple example, we can easily reduce a complex computation if can do reduce its individual parts first. For instance, if we want to compute "mod 10", then we are effectively talking about keeping only the ones digit from the number. So for instance we can do:

$$45322 \times 343523 \times 34519 \equiv 2 \times 3 \times 9 \equiv 54 \equiv 4 \bmod 10$$

As another example, let us try to compute $2^{10} \bmod 5$:

$$2^3 = 8 \equiv 3 \bmod 5$$

$$2^4 = 8 \times 2 = 3 \times 2 = 6 \equiv 1 \bmod 5$$

$$2^8 = 2^4 \times 2^4 \equiv 1 \times 1 = 1 \bmod 5$$

$$2^10 = 2^8 \times 2^2 \equiv 1 \times 4 = 4 \bmod 5$$

In fact we can efficiently compute powers with very large exponents very efficiently, if we work modulo a number.

This technique can give rise to some really nice divisibility tests:

> A number is congruent to the sum of its digits modulo 9.
>
> Consequently a number is divisible by 9 if and only if the sum of its digits is.
>
> A number is congruent to the alternating sum of its digits modulo 11.
>
> Consequently a number is divisible by 11 if and only if the alternating sum of its digits is.

For example, 3412458 is divisible by 9 since $8 + 5 + 4 + 2 + 1 + 4 + 3 = 27$. It is not divisible by 11 since $8 - 5 + 4 - 2 + 1 - 4 + 3 = 5$.

> Question: Can we have two numbers that are not $\equiv 0 \mod n$ but whose product is $\equiv 0 \mod n$?