

THE JOY OF NUMBERS

1. POWERS AND CONGRUENCE MODULE m

We first solve homework from last time.

(1.1) **Proposition.** $911^{853} \equiv 3 \pmod{4}$.

Proof. (Alex) $911 \equiv 3 \pmod{4}$ and $3^2 \equiv 1 \pmod{4}$. So we have

$$911^{853} \equiv 3^{853} \equiv 3^{2 \cdot 426 + 1} \equiv (3^2)^{426} 3 \equiv 3 \pmod{4}.$$

□

(1.2) **Proposition.** $3^{90} \equiv 9 \pmod{20}$.

Proof. (Danny) $3^4 \equiv 1 \pmod{20}$. So,

$$3^{90} \equiv 3^{4 \cdot 22 + 2} \equiv (3^4)^{22} 3^2 \equiv 9 \pmod{20}$$

□

(1.3) **Proposition.** Let N be a number, write $N = d_n \dots d_1$, meaning that

$$N = d_1 + d_2 \cdot 10 + d_3 \cdot 10^2 + \dots + d_n \cdot 10^{n-1}.$$

Prove that N is divisible by 3 if and only if $\sum d_i$ is divisible by 3.

Proof. (Chris) Being divisible by 3 means that a number is congruent to zero modulo 3. So what we really need to prove is the following

$$N \equiv 0 \pmod{3} \text{ if and only if } \sum d_i \equiv 0 \pmod{3}.$$

For this notice that $10 \equiv 1 \pmod{3}$ and therefore $10^n \equiv 1^n \equiv 1 \pmod{3}$ for all positive integers n . So $N \equiv 0 \pmod{3}$ if and only if $d_1 + d_2 \cdot 10 + d_3 \cdot 10^2 + \dots + d_n \cdot 10^{n-1} \equiv 0 \pmod{3}$ if and only if $d_1 + \dots + d_n \equiv 0 \pmod{3}$. □

Eric came up with other divisibility conditions.

(1.4) **Exercise.** Let N be a positive integer, write $N = d_n \dots d_1$ so that $N = d_1 + d_2 \cdot 10 + \dots + d_n \cdot 10^{n-1}$. Show that N is divisible by 4 if and only if $d_1 + d_2 \cdot 10$ is divisible by 4.

(1.5) **Exercise.** Let N be a positive integer, write $N = d_n \dots d_1$ so that $N = d_1 + d_2 \cdot 10 + \dots + d_n \cdot 10^{n-1}$. Show that N is divisible by 11 if and only if $\sum_{i=1}^n (-1)^i d_i$ is divisible by 11.

And also Chris:

(1.6) **Exercise.** (This one was hard to write down) Let N be a positive integer, write $N = d_n \dots d_1$ so that $N = d_1 + d_2 \cdot 10 + \dots + d_n \cdot 10^{n-1}$. Show that N is divisible by 37

We moved on the real subject of the day: the powers. We first filled a table:

m	list of all a with $1 \leq a \leq m - 1$ and $a^k \equiv 1 \pmod{m}$ for some positive k (the smallest such k is in parenthesis)
2	1 ($k = 1$)
3	1 ($k = 1$), 2 ($k = 2$)
4	1 ($k = 1$), 3 ($k = 2$)
5	1 ($k = 1$), 2 ($k = 4$), 3 ($k = 4$), 4 ($k = 2$)
6	1 ($k = 1$), 5 ($k = 2$)
7	1 ($k = 1$), 2 ($k = 3$), 3 ($k = 6$), 4 ($k = 3$), 5 ($k = 6$), 6 ($k = 2$)
8	1 ($k = 1$), 3 ($k = 2$), 5 ($k = 2$), 7 ($k = 2$)
9	1 ($k = 1$), 2 ($k = 6$), 4 ($k = 3$), 5 ($k = 6$), 7 ($k = 3$), 8 ($k = 2$)

It took a while but we finally formulated the following:

(1.7) **Conjecture.** Let m be an integer. If $\gcd(a, m) = 1$ then there exists a k such that $a^k \equiv 1 \pmod{m}$.

And then the usual questions came up:

- (1.8) **Question.**
- (1) Is the converse true? Meaning, if there exists a k such that $a^k \equiv 1 \pmod{m}$ must then $\gcd(a, m) = 1$?
 - (2) If $\gcd(a, m) = 1$, what is the smallest k such that $a^k \equiv 1 \pmod{m}$?