Lesson 20

Modular arithmetic : application

Th $\forall n \in \mathbb{Z}$ 3 divides n^3+2n

Proof: Pet's rewrite it as $\forall n \in \mathbb{Z}$ $n^3+2n \equiv 0 \mod 3$

1) If $n \equiv 0 \mod 3$ then $n^3+2n \equiv 0^3+2\cdot 0 \equiv 0 \mod 3$
2) If $n \equiv 1 \mod 3$ then $n^3+2n \equiv 1^3+2\cdot 1 = 3 \equiv 0 \mod 3$
3) If $n \equiv 2 \mod 3$ then $n^3+2n \equiv 2^3+2\cdot 2 = 12 \equiv 0 \mod 3$

Question: is 98765321 divisible by 3?

$98765321 = 1 + 2\cdot 10 \cdot 3\cdot 10^2 + 4\cdot 10^3 + 5\cdot 10^4 + 6\cdot 10^5 + 7\cdot 10^6 + 8\cdot 10^7 + 9\cdot 10^8 \equiv 1+2+3+4+5+6+7+8+9$ (since $10 \equiv 1 \mod 3$ so $10^n \equiv 1 \mod 3$ for $n \geq 0$) $\equiv 0 \mod 3$ yes it is divisible.

Th: If $a_k a_{k-1} \cdots a_0$ is the decimal representation of $n \in \mathbb{Z}^+$ then 3 divides n <=> $a_k + a_{k-1} + \cdots + a_0 + a_1 \equiv 0 \mod 3$

Diophantine equations

Example $x^2 - 7y^2 = 73$ has no integer solutions.

Idea work mod 7. Why 7? $7y^2 \equiv_7 0$ so one variable disappears

Assume by contradiction that $x_1^2 - 7y_1^2 = 73$ then we must have $x_1^2 - 7y_1^2 \equiv_7 73$ so

$x_1^2 \equiv 3 \mod 7$ but

if $x_1 \equiv_7 0$	$x_1^2 \equiv_7 0$
if $x_1 \equiv_7 1$	$x_1^2 \equiv_7 1$
if $x_1 \equiv_7 2$	$x_1^2 \equiv_7 4$
if $x_1 \equiv_7 3$	$x_1^2 \equiv_7 2$
if $x_1 \equiv_7 4$	$x_1^2 \equiv_7 2$
if $x_1 \equiv_7 5$	$x_1^2 \equiv_7 4$
if $x_1 \equiv_7 6$	$x_1^2 \equiv_7 1$

There is no x_1 s.t $x_1^2 \equiv_7 3$, contradiction

Note: to prove that an equation has no solution in $\mathbb{Z}$, you can try to choose m

and show the equation has no solution mod m.

The other way around does not work: an equation may have a solution mod m, for some m, but no solution in $\mathbb{Z}$. It may even have solution mod m for all $m \geq 2$ and no solution in $\mathbb{Z}$.

Question: what is the last digit (unit digit) of 3^{100}? We can translate this as what is 3^{100} mod 10?

$$3^{100} = 9^{50} \equiv_{10} (-1)^{50} \equiv_{10} 1$$

3^{100} ends in 1

Systematic way to compute powers mod m by repeated squaring:

Example Compute $3^{37} \bmod 53$

(1) Write 37 as sum of powers of 2

$37 = 32 + 4 + 1$

(2) Keep computing powers of 3 mod 53 by squaring up to power 32

$3^2 \equiv_{53} 9$

$3^4 = (3^2)^2 = 81 \equiv_{53} 28$

$3^8 = 81^2 \equiv_{53} 28^2 = 784 \equiv_{53} 42$

because calculator says: $784 \div 53 = 14.79\ldots$

and $784 - 53 \cdot 14 = 42$

$3^{16} \equiv_{53} 42^2 = 1764 \equiv_{53} 15$

$3^{32} \equiv_{53} 15^2 = 225 \equiv_{53} 13$

(3) Compute 3^{37}

$3^{37} = 3^{32+4+1} = 3^{32} \cdot 3^4 \cdot 3 \equiv_{53} 13 \cdot 28 \cdot 3$

$= 1092 \equiv_{53} 32$