MATHEMATICAL ENRICHMENT UCD

Sat March 7th 2020

Kevin Hutchinson: Number Theory

[No session next Saturday March 14th]

Some problems from last time.

1. Find $\gcd(2^8+1, 2^{32}+1)$. Express it as $s\cdot(2^8+1) + t\cdot(2^{32}+1)$

[First suppose $d \mid 2^8+1$ and $d \mid 2^{32}+1$.

$\Rightarrow d \mid (2^8+1)(2^8-1) = 2^{16}-1$

$\Rightarrow d \mid (2^{16}-1)(2^{16}+1) = 2^{32}-1$ $\Rightarrow d = 1$]

Find s, t: ...

[Euclid's algorithm. $(a,b) = ?$ If $b = qa + r$ then $(a,b) = (a,r)$]

Eg

$$2^{32}+1 = 2^{24}\cdot(2^8+1) - (2^{24}-1)$$
$$2^{24}-1 = 2^{16}\cdot(2^8+1) - (2^{16}+1)$$
$$2^{16}+1 = 2^8\cdot(2^8+1) - (2^8-1)$$
$$2^8+1 = 1\cdot(2^8-1) + 2$$
$$2^8-1 = (2^7-1)\cdot 2 + 1$$

$\Rightarrow$ go backwards:

$$(2^{31} - 2^{23} + 2^{15} - 2^7 + 1)\cdot(2^8+1) - 2^7\cdot(2^{32}+1) = 1$$

2. $(m, n) = 1 \quad (m^2 - n^2, 2mn) = 1$ or 2

Easy $\gcd = 2 \iff$ both odd.

Let p be any odd prime.

[Recall p prime and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Generally $p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i$ for some i.

i.e. $p \mid a^n \Rightarrow p \mid a$.]

p odd and $p \mid 2mn \Rightarrow p \mid m$ or $p \mid n$.

If $p \mid m^2 - n^2$ and $p \mid m \Rightarrow p \mid n^2 \Rightarrow p \mid n$

$\Rightarrow p \nmid m \rightarrow\leftarrow$

not possible.

Similarly, there is no odd prime p s.t.

$p \mid n$ and $p \mid m^2 - n^2$

---

3. $(m, n) = d \Rightarrow$ for any $a > 1$

$$(a^m - 1, a^n - 1) = a^d - 1.$$

Solution: $a^t - 1 = (a-1)(1 + a + \cdots + a^{t-1})$

$d \mid m \Rightarrow$ $m = d\ell$ $\quad a^m - 1 = a^{d\ell} - 1 = (a^d)^\ell - 1$

$= (a^d - 1)(1 + a^d + \cdots + a^{d(\ell-1)})$

So $d \mid m \Rightarrow a^d - 1 \mid a^m - 1$.

So $a^d - 1$ is a common divisor of $a^m - 1$ & $a^n - 1$.

GCD? Show $a^d - 1 = S \cdot (a^m - 1) + T \cdot (a^n - 1)$

$(m,n) = d \Rightarrow sm - tn = d$

for some $s, t \geq 0$.

So $d + tn = sm$

$\Rightarrow a^d \cdot a^{tn} = a^{sm}$

$a^d \cdot (a^{tn} - 1) = a^{sm} - a^d = (a^{sm} - 1) - (a^d - 1)$

So $a^d - 1 = \underbrace{(a^{sm} - 1)}_{\text{multiple of } a^m - 1} - a^d \cdot \underbrace{(a^{tn} - 1)}_{\text{multiple of } a^n - 1}$

Done

Modulo Arithmetic / Congruences

Recall $m > 1$

Def^n $a \equiv b \pmod m$ means

(i) $m \mid a - b$

$\iff$ (ii) $a = b + mt$ for some m

$\iff$ (iii) a and b leave same remainder on division by m.

Examples $23 \equiv 11 \mod 12$

$23 \equiv -1 \mod 12$

$365 \equiv 1 \mod 7$

Useful because:

Theorem Suppose $a \equiv b \mod m$ and $c \equiv d \mod m$

Then (1) $a + c \equiv b + d \mod m$

(2) $ac \equiv bd \mod m$

(3) $a^n \equiv b^n \mod m$ for any $n \geq 1$

Proof. $ac - bd = (a-b)c + b(c-d)$

$\uparrow$ div by m $\quad\quad$ $\uparrow$ div by m.

Examples Show that $11 \cdot 7^n + 4$ is divisible by 3 for every n.

Solution $11 \equiv 2,\ 7 \equiv 1,\ 4 \equiv 1 \mod 3$

$$\Rightarrow \quad 11 \cdot 7^n + 4 \equiv 2 \cdot 1^n + 1 \mod 3$$
$$\equiv 3 \equiv 0 \mod 3 \quad ✓$$

Find the remainder of 5^{1000} on division by 12.

Solution $5^2 = 25 \equiv 1 \pmod{12}$

$$5^{1000} = (5^2)^{500} \equiv 1^{500} \equiv 1 \mod 12.$$

Answer : 1

Show that the number $2 \cdot 13^n + 1$ is never a prime number

Modulo 3 this is $2 \cdot 1^n + 1 \equiv 3 \equiv 0$ mod 3.

So $3 \mid 2 \cdot 13^n + 1$ always.

Recall

$N > 1$ decimal expansion $a_t a_{t-1} \cdots a_1 a_0$

Then
$$N \equiv a_0 + a_1 + a_2 + \cdots + a_t \mod 9$$
$$N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^t a_t \mod 11.$$

Why? $\quad N = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^t a_t$

$10 \equiv 1 \mod 9$

$10 \equiv -1 \mod 11$

Moscow 1964

(a) Show $7 \mid 2^n - 1 \iff 3 \mid n.$

$[\Leftarrow \quad 3 \mid n \Rightarrow n = 3t \Rightarrow 2^n - 1 = 2^{3t} - 1 = (2^3-1)(1+2^3+\cdots)]$

i.e. $2^n \equiv 1 \mod 7$

(Alternatively
$2^3 \equiv 1 \mod 7 \Rightarrow (2^3)^t \equiv 1^t \equiv 1 \mod 7$

Given any n, write $n = 3t + r$ $\quad r = 0, 1,$ or $2.$
$(n \equiv r \bmod 3)$

$$2^n = 2^{3t} \cdot 2^r \equiv 1 \cdot 2^r \equiv 2^r \mod 7$$

If $r = 1$, $\quad 2^n \equiv 2 \not\equiv 0 \mod 7 \Rightarrow 7 \nmid 2^n - 1.$

If $r = 2$, $\quad 2^n \equiv 2^2 \equiv 4 \not\equiv 0 \Rightarrow 7 \nmid 2^n - 1.$

Recall problem from last time:

$(m,n) = d \Rightarrow (a^m - 1, a^n - 1) = a^d - 1.$

$[a^d \equiv 1 \mod (a^d - 1) \Rightarrow a^{dt} \equiv 1^t \equiv 1 \mod (a^d - 1)$

$\Rightarrow a^d - 1 \mid a^{dt} - 1 \;]$

Conversely, we show if $\ell \mid a^m - 1,\ a^n - 1$ then $\ell \mid a^d - 1$.

$\Downarrow$

$a^m \equiv 1 \mod \ell,\quad a^n \equiv 1 \mod \ell$

We have $\quad d = sn - tm \quad$ ie $\quad d + tm = sn$

$\Rightarrow \quad a^d \cdot a^{tm} \equiv a^{sn} \mod \ell$

$\Rightarrow \quad a^d \cdot 1 \equiv 1 \mod \ell$ ✓.

Moscow 1964

(b) Show that $2^n + 1$ is <u>never</u> divisible by 7.

From part (a) we have seen $\boxed{2^n \equiv \underset{2^0}{1}, \underset{2^1}{2}, \underset{2^2}{4}} \mod 7$

$\Rightarrow \quad 2^n + 1 \equiv 2, 3, 5 \mod 7$

<u>Example</u> x, y odd numbers.

Show $x^2 + y^2$ is not a square.

<u>Modulo 4:</u> $\quad x, y$ odd $\Rightarrow x^2 \equiv y^2 \equiv 1 \mod 4$.

$(x$ odd $\Rightarrow x \equiv 1, 3 \mod 4$

$\Rightarrow x^2 \equiv 1, 9 \mod 4 \Rightarrow x^2 \equiv 1 \mod 4)$

x_0 even $\Rightarrow x^2 \equiv 0 \mod 4$.

$x^2 + y^2 \equiv 1 + 1 \equiv 2 \mod 4$

But $z^2 \equiv 0, 1 \mod 4$ always.

So $x^2 + y^2$ is not a square

<u>Example</u> Show that the equation

$$x^2 - 7y = 66$$

has no integer solutions.

<u>Solution</u> Modulo 7:

$$x^2 \equiv 66 \equiv 3 \text{ modulo } 7.$$

$$x \equiv 0, \pm 1, \pm 2, \pm 3 \mod 7$$

$$\Rightarrow x^2 \equiv 0, 1, 4, 2 \mod 7$$

So $x^2 \not\equiv 3 \mod 7$

<u>Example</u> Prove that $a^5 - a$ is always divisible by 5.

<u>Solution</u> i.e. show $a^5 \equiv a \mod 5$ for all a.

$$a \equiv 0, 1, 2, -2, -1 \mod 5.$$

$a \equiv 0 \Rightarrow a^5 \equiv 0^5 \equiv 0 \equiv a$ ✓

$a \equiv 1 \Rightarrow a^5 \equiv 1^5 \equiv 1 \equiv a$ ✓

$a \equiv 2 \Rightarrow a^5 = 32 \equiv 2 \equiv a \mod 5$

$a \equiv -2 \Rightarrow a^5 \equiv -32 \equiv -2 \equiv a \mod 5$ ✓.

$a \equiv -1 \Rightarrow a^5 \equiv (-1)^5 = -1 \equiv a \mod 5$

Example Calculate the remainder of

$$11^{11^{11}}$$ on division by 13.

[General Idea To calculate $a^{BIG} \mod m$.

1st find (small) d with $a^d \equiv 1 \mod m$.

If $BIG = td + r$ we have

$$a^{BIG} \equiv a^r \mod m.$$

i.e. if $BIG \equiv r \mod d$, $a^{BIG} \equiv a^r \mod m$].

1st solve $11^d \equiv 1 \mod 13$: Look at powers of 11 modulo 13

$11 \equiv -2 \implies 11^2 \equiv (-2)^2 \equiv 4 \mod 13$

$11^4 \equiv 4^2 \equiv 16 \equiv 3 \mod 13$

$\implies 11^6 = 11^2 \cdot 11^4 = 4 \cdot 3 \equiv -1 \mod 13.$

$\therefore$ $11^{12} \equiv 1 \mod 13.$ Take $d = 12$.

Now we calculate $11^{11} \mod 12$

$11 \equiv -1 \implies 11^{11} = (-1)^{11} \equiv -1 \mod 12$

i.e. $11^{11} \equiv 11 \mod 12.$

$\therefore$ $11^{11^{11}} \equiv 11^{11} \mod 13$

$11^{11} \equiv -11^5 \equiv -3 \cdot 11 \equiv -3 \cdot -2 \equiv 6 \mod 13.$

$(11^6 = \ldots$ Answer: 6

Some Exercises

(1) Calculate the last digit of $13^{13^{13}}$

(2) Use Euclid's algorithm to solve

$$33x \equiv 1 \mod 59$$
$$(1 \le x \le 58)$$

(3) Show $5 \cdot 23^n + 14 \cdot 43^n$

is neither a square nor a fifth power for all n.

(4) (IMO Bulgaria 1975)

A = sum of the digits of 4444^{4444}

B = sum of the digits of A.

C = sum of the digits of B.

Find the precise value of C.