Mathematical Enrichment — Sat March 29th

Dr. Kevin Hutchinson

Recall

1. m odd positive number.
Show that some positive power of 2 leaves remainder 1 on division by m.

2. Show that there is an infinite sequence
$$2^{n_1}-1 < 2^{n_2}-1 < 2^{n_3}-1 < \cdots\cdots$$
which is pairwise relatively prime

Sol^n
Let $a_1, a_2, a_3, \ldots$ be this sequence of numbers.

Take $a_1 = 2^2-1 = 3$.

Now suppose we have constructed $a_1, \ldots, a_k$.

We show to extend this sequence by one more term:

[Aside: Idea – Use Euclid's strategy.

$$a_{k+1} = {}_2Na_1\cdots a_k + 1$$

Wait $\quad$ $\parallel$

$$2^r - 1 = 2Na_1\cdots a_k + 1$$

$$\therefore \quad 2^r - 2 = 2Na_1\cdots a_k \Leftrightarrow 2^{r-1} - 1 = Na_1\cdots a_k$$

need $\quad 2^{r-1} = Na_1\ldots a_k + 1$]

By 1. there exists $s \geq 1$ such that

$$2^s = Na_1\cdots a_k + 1.$$

So $$2^{s+1} = 2Na_1\cdots a_k + 2$$

$$\therefore \quad 2^{s+1} - 1 = 2Na_1\cdots a_k + 1$$

Let $a_{k+1} = 2^{s+1} - 1$. Done

Back to 1: m odd.

Consider the numbers $2, 2^2, \ldots, 2^m, 2^{m+1}$

By the "pigeonhole principle" some pair must have the same remainder on division by m.

$\therefore$ 2^s and 2^r $(r < s)$ have the same remainder

$\overset{(**)}{\Rightarrow}$ $2^s - 2^r$ is divisible by m.

So $$m \mid 2^s - 2^r = \underbrace{2^r}_{a} \cdot (\underbrace{2^{s-r} - 1}_{b})$$

But m is odd. So$^{(*)}$ $m \mid 2^{s-r} - 1 = 2^d - 1$

$2^d - 1 = mt$ for some integer t.

$$\therefore \quad \boxed{2^d = mt + 1}$$

(*) In general: If $m \mid ab$ and suppose $(m,a) = 1$ then $m \mid b$. (Proof: difficult).

We say a is congruent to b modulo m if

a and b have the same remainder on division by m.

equivalently: if $m \mid a-b$.

(We write

$a \equiv b \pmod{m}$.)

"modulus"

We've just shown: If m is odd. Then there is some $d \geq 1$ such that $2^d \equiv 1 \bmod m$.

Algebra of congruences

Suppose $a_1 \equiv b_1 \bmod m$ and $a_2 \equiv b_2 \bmod m$

Then $a_1 + a_2 \equiv b_1 + b_2 \bmod m$.

$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod m$

If $a \equiv b \bmod m$ then $a^n \equiv b^n \bmod m$.

If $(a,m) = 1$ then $a^d \equiv 1 \bmod m$ for some $d \geq 1$ [Exercise: Copy the argument with $a=2$ above]

Eg. $2^5 \equiv 1 \bmod 31$.

What is the remainder of 2^{487} on division by 31?

Note that $2^5 \equiv 1 \bmod 31 \Rightarrow$

$(2^5)^n \equiv 1^n \bmod 31$

So $2^{5n} \equiv 1 \bmod 31$ for any n.

$487 = 485 + 2.$

So $2^{487} = 2^{485} \cdot 2^2 \equiv 2^{485} \cdot 2^2 \bmod 31$

$\equiv 1 \cdot 4 \bmod 31$

$\equiv 4 \bmod 31$

Answer: 4

What's ~~the smallest~~ a power of 2 congruent to $1 \bmod 33$?

Sol^n $2^5 \equiv -1 \bmod 33.$ $\left(33 \mid 2^5 - (-1) \quad \checkmark \right)$

$\therefore$ $(2^5)^2 \equiv (-1)^2 \bmod 33$

ie $2^{10} \equiv 1 \bmod 33$

Fermat's Little Theorem

If p is prime and if a is any integer then $a^p \equiv a \bmod p$ $\quad (p \mid a^p - a)$.

(Pf: Exercise).

If $(a,p) = 1$ (since p is prime this just means $p \nmid a$)

then $a^{p-1} \equiv 1 \bmod p.$

($p \mid a^p - a = a \cdot (a^{p-1} - 1)$ and $(p,a) = 1$

$\Rightarrow p \mid a^{p-1} - 1.$)

$p = 31$ is prime. $(p-1 = 30$

FLT tells us $2^{30} \equiv 1 \mod 31.$

(in fact $2^5 \equiv 1 \mod 31$).

but also $3^{30} \equiv 1 \mod 31$

FLT tell us .. $4^{30} \equiv 1 \mod 31$

Find the remainder of 5^{20} on division by 17.

Sol^n By FLT $5^{16} \equiv 1 \mod 17$

$\Rightarrow 5^{20} = 5^{16} \cdot 5^4 \equiv 5^4 \mod 17$

$5^2 \equiv 8$

$\Rightarrow 5^4 \equiv 8^2 \equiv 64 \equiv 13 \mod 17.$

Ans: 13

Order of a modulo m

Suppose $(a, m) = 1$.

Then we know $a^n \equiv 1 \mod m$ for some $n \geq 1$.

It follows $a^{nt} \equiv 1 \mod m$ for any $t \geq 1$

$a^{nt} = (a^n)^t$

Definition The order of a modulo m is the smallest $d > 0$ for which $a^d \equiv 1 \mod m$.

<u>Lemma</u> Suppose $(a,m)=1$ and d is the order of a mod m.

Then if $a^n \equiv 1 \bmod m$, n must be a multiple of d.

<u>Proof:</u> $n = dt + r$ where r, t are integers and $0 \leq r < d$

(We want to show $r=0$.)

$$a^n \equiv 1 \bmod m$$

$$\therefore \quad a^{dt+r} \equiv 1 \bmod m.$$

But $a^{dt+r} = a^{dt} \cdot a^r \equiv 1 \cdot a^r \equiv a^r \bmod m.$

Comparing, $a^r \equiv 1 \bmod m$

By <u>minimality</u> of d, this means $r=0$.

<u>Some applications</u>

<u>1.</u> Find the order of 2 modulo 33.

<u>Sol^n</u> Let d be this order.

$$2^{10} \equiv 1 \bmod 33$$

$\therefore$ By the Lemma, $d \mid 10 \Rightarrow d = \underbrace{\cancel{1}, \cancel{2}, \cancel{5}}_{\text{too small}}, 10$

So $d=10$

Example

Find a prime divisor of

$$2^{32}+1 = 429\,496\,7297$$

Sol^n Let p be a prime divisor.

$$p \mid 2^{32}+1$$

$$\Rightarrow \quad 2^{32} \equiv -1 \mod p$$

$$\Rightarrow \quad 2^{64} \equiv 1 \mod p$$

Let d = order of 2 modulo p.

$$d \mid 64, \ d \nmid 32 \ \Rightarrow \ \underline{\underline{d = 64}}$$

But FLT says $2^{p-1} \equiv 1 \mod p$.

By our Lemma, $64 \mid p-1$ i.e.

$$\boxed{p \equiv 1 \mod 64}$$

i.e. $p = 64t + 1$ for some $t \geq 1$.

~~65~~

primes of form $64t+1$

works

$\cancel{193}$, $\cancel{449}$, $\cancel{577}$, $\boxed{641}$, ...

In fact $2^{32}+1 = 641 \cdot \underbrace{6700417}_{\text{also prime.}}$

I.M.O. 1990

Find all positive integers $n > 1$ such that

$$\frac{2^n+1}{n^2} \text{ is an integer.}$$

(Start of)
Solution: First $n = 3$ works. (1 pt).

Note any solution must be odd

The condition can be expressed:

$$2^n \equiv -1 \bmod n^2$$

So $2^{2n} \equiv 1 \bmod n^2$.

~~Let d = order of 2 mod n^2. Then $d \mid 2n$.~~

Let p be a prime dividing n.

Then $2^{2n} \equiv 1 \bmod p$

By FLT, $2^{p-1} \equiv 1 \bmod p$

Let d be the order of 2 mod p.

$d \mid 2n$ and $d \mid p-1$.

Let p = smallest prime dividing n.

$d = 2r$ where $r \mid n$ and $r \mid p-1$
$\Rightarrow r < p$

By minimality of p, $r = 1$. and hence $d = 2$.

So $2^2 \equiv 1 \bmod p \Rightarrow p \mid 2^2 - 1 \Rightarrow \boxed{p = 3}$

Finish off solution: ~~Let q~~ Take q to be the next smallest prime .. and deduce there is no such q.

Finally We know $n = 3^a$.

Show only $a=1$ works