Number Theory

2010-10-05

2

Primes of form $4m-1$: If only finitely many: $p_1, \dots, p_n$.

Let $N = 4p_1p_2\cdots p_n - 1$.

Not prime $\Rightarrow$ has prime dividing it, of form $4k-1$ since if all of form $4k+1$, $N \equiv 4k+1$.

$\Rightarrow$ one of the p_i $\ast$.

Remainder mod 2 of $((\sim 27 \times 12110 + 10721 \times 23) \times 3$

2^{29} Remainder mod 9 = sum of digits mod 9.

Since sum of digits: $N = \underline{d_t \cdots d_1 d_0} = d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^t d_t$.

So ~~(~~mod 9) $N \equiv d_0 + d_1 + \cdots$ (sum of digits)

since $10 \equiv 1 \pmod 9$.

2^{29} mod 9.

$2^{29} = \cancel{2^{16} \times 2^8 \times 2^4 \times 2^1}$ $\quad (2^7)^4 \times 2$

5 2

(9)

$9 \overline{)128}$ 14, 38, 36, 2.

$\rightarrow 2^4 \times 2 = 32 \rightarrow 5$ mod 9.

$= 4$ 4 is missing

$\boxed{536870912}$

But if all 10 digits: $0\underline{12345\dots9}$ sum is $9 \times 5 = 45 \equiv 0$

$\underline{40!}$ How many 0s? #5's is limiting factor.

5, 10, 15, 20, 25, 30, 35, 40

+1 +1 +1 +1 +2 +1 +1 +1

$= 9 = \left\lfloor \frac{40}{5} \right\rfloor + \left\lfloor \frac{40}{5^2} \right\rfloor + \cdots$

So all last are 0's.

Front: Mod 999999, is sum of all 6-segments, since replace $1000000 \equiv 1 \pmod{999999}$

$999999 = 9 \times 111 \times 1001$

$= 9 \times 3 \times 37 \times 7 \times \underbrace{143}_{13 \times 11} \rightsquigarrow 0$

~~283 247~~ ~~887 734~~

272 000
115 894
269 596
346 611
897 734
+ 283 247

⋰

2010-10-05

(3)

2000/A2.

0^2+ sqr, sqr $+1^2$, sum of sqs

odd odd even

So either $a^2+b^2 = c^2+2$ ~~mod 4: if $c^2=0,1 \Rightarrow c^2+2=2,3$.~~

or $a^2+b^2 = c^2-1$. infinitely often.

find $= (c+1)(c-1)$

$b^2+1 = c^2-a^2 = (c+a)(c-a)$,

so find nonprime b^2+1, odd, $= rs$, $r<s$

$\frac{r+s}{2}$, $\frac{s-r}{2}$.

0 ... n^2

$\frac{n^2}{2}$ choices of pair, sum is in $0 \ldots 2n^2$.

$\left(\frac{n}{2}\right)^2$ choices of odd, even. Sum's in $0 \ldots 2n^2$, but odd $\to n^2$.

$2a^2 = c^2+2$?

$c = 2c'$.

$2a^2 = 4c'^2+2$

$a^2 = 2c'^2+1$,

$a^2 = 8c^2+1$,

$\forall$ nonprime odd $b^2+1, \ldots$

rs, $r<s$, both odd

$c+a = s$ $\quad c = \frac{s+r}{2}$, int

$c-a = r$. $\quad a = \frac{s-r}{2}$, int

gives a^2+b^2 $=$ some c^2-1, then c^2+0^2, c^2+1^2.

Produces diff if bigger.

s is bigger

So just find such b^2+1 keeps bigger,

so $\frac{s+r}{2}$ bigger

(min at $\sqrt{b^2+1}$.)

Why there is nonprime eventually.

if ~~every~~ $(\text{even})^2+1$ is prime...

Then ~~$c^2+0^2 = a^2+b^2$~~

$c^2-a^2 = sr = b^2+1$.

$c^2-1 = a^2+b^2$

-1 is QR. mod some prime

Mod 5, say. $2^2=4$.

So $\left[-2 \pmod 5\right]^2+1$ is div by 5.

pick one which is even.

2000/B2 $\quad \frac{\gcd(m,n)}{n}\binom{n}{m} = \frac{am+bn}{n}\binom{n}{m} \Leftrightarrow a\frac{m}{n}\cdot\binom{n}{m} = a\frac{m}{n} - \frac{n}{m}\binom{n-1}{m-1}$

$n \geq m$. always ok.

Why $\gcd(m,n) = rm+sn$ for some r,s

$\overset{\|}{g}$ Consider all $\mathbb{Z}m+\mathbb{Z}n$, and let $h=$ smallest positive integer there

$an+bm$.

Clearly, $g|h$.

big-small

Euclidean Alg: $\gcd(m,n) = \gcd(n, n-m)$ ... until $\gcd(m,0)$

largest number keeps shrinking unless smaller is 0.

$\gcd(k,0)=k$.

Lem $\gcd(m,n) = \gcd(m-kn, n)$

Suffi show any f dividing LHS divides RHS. YES

m,n $\quad m-kn, n$

2010-10-05

(4)

GA 727

$b > a$

$\gcd(n^a - 1, n^b - 1)$

Euclid: $\left[n^a - 1, (n^b - 1) - n^{b-a}(n^a - 1)\right]$

$= \cancel{n^b} - 1 \cancel{- n^b} + n^{b-a}$

$= n^{b-a} - 1$

So follow Euclid Alg to gcd a, b.

final step in gcd (a, b) is g vs 0.

$\left[n^{\gcd(a,b)} - 1, \underset{\underset{0}{\|}}{n^0 - 1}\right]$

As desired.

V 2006/3

$F(n) = F(n-1) + F(n-2)$

$= F(n-2) + F(n-3) + F(n-2) = \boxed{2F(n-2) + F(n-3)}$

$F(n) \equiv F(n-3)$, $2006 \equiv 2$.

$= 2(F(n-3) + F(n-4)) + F(n-3)$

$= 3F(n-3) + 2F(n-4)$

$= 3[F(n-4) + F(n-5)] + 2F(n-4)$

$= 5F(n-4) + 3F(n-5)$

So $\boxed{\bmod 5}$, $F(n) \equiv 3F(n-5)$

$\frac{2005}{5} = 401$

$F(2006) \underset{(5)}{\equiv} 3^{401} F(1)$, $F(1) = 1$

3^{401} mod 5. $\equiv 3 \pmod 5$

k	3^k (5)
0	1
1	3
2	4
3	2
4	1
5	3

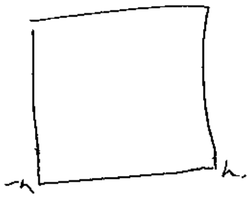
So ends with 3 or 8.

even or odd?

$F(2006) \equiv F(2) \equiv 1$. odd

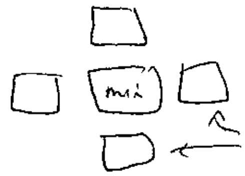
2010-10-05
(5)

GA $\mathbb{Z}^2$.



Def. $m(n)$ = smallest # in:

If min is inside (in the $(n-1)$),



$\Rightarrow$ all 4 around are equal to it

one of these is another inside square

$\Rightarrow$ whole ~~inside is the min~~ square.

Now what of $m(1), m(2), m(3), \ldots$

this seq is decr. If $m(k) = m(k+1)$, then whole ~~sq~~ $k+1$ $\boxed{\text{equal}}$

But must have equality infinitely often, since $m(1)$ finite

So all eqh

1999 Putnam $n \mid 2^n + 1$.

$2^n \bmod n$.

$n q = 2^n + 1$, odd

q always odd

$(2k+1) q = 2^{2k+1} + 1$

$2kq + q = 2^{2k+1} + 1$

$2^n = (1+1)^n = \cancel{4^n} \ldots$

$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \cancel{\binom{n}{n}}$

$n=3$: $1 + 3 + 3$

$n \mid 2^n - 1$

$= \cancel{\ldots} \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$ 1

$p \nmid 2^p - 1$.

Fermat little thm: $2^p \equiv 2 \pmod p$

$2^{pq} - 1$?

$2^{pq} \equiv 2^q \pmod p$
could be 1

?

$n \mid 2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}$.

1
2
4
8
16