MATH 4410
Nate Stott A02386053

Quiz #9; Due 11:59 pm, 4/3/2024

1. Prove that if $2^N + 1$ is prime, then N must be a power of 2.

   Let p be a prime

$$2^N + 1 = p$$
$$2^N = p - 1$$
$$N = \log_2 (p - 1)$$

   Therefore, if $2^N + 1$ is prime, then N must be a power of 2 (we only care about the $p - 1$'s that give us a whole number and the only p-1's that give us a whole number are powers of 2! (note that is an explanation-point, not a factorial.)).

2. Let f_n denote the n^{th} *Fermat Number*, defined by $f_n = 2^{2^n} + 1$.

(a) Prove that if $n < m$, $f_n \perp f_m$.

$$f_m = 2^{2^m} + 1$$
$$f_n = 2^{2^n} + 1$$

$$f_m = 2^{2^m} + 1$$

Then n can be $m-1, m-2, ...0$

Let m be 3

$$f_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$
$$f_{3-1} = 2^{2^{3-1}} + 1 = 2^4 + 1 = 17$$
$$f_{3-2} = 2^{2^{3-2}} + 1 = 2^2 + 1 = 5$$
$$f_{3-3} = 2^{2^{3-3}} + 1 = 2^1 + 1 = 3$$

So I need to look at these guys 2^8, 2^4, 2^2, 2^1

Well, none of them are relatively prime to each other because they are powers of 2. But when you add a 1 then the numbers became relatively prime. Let's investigate this.

3 is prime
5 is prime
17 is prime
257 is prime
65537 is prime
4294967297 is not prime since $641 * 6700417$ but those numbers are prime.

So all the Fermat numbers below f_m have unique prime factorizations

Therefore, if $n < m$, $f_n \perp f_m$

(b) Prove that $f_n - 2 = f_0 \cdot f_1 \cdot f_2 \cdots f_{n-1}$, for $n \geq 1$ and $f_0 = 3$.

$$f_n = 2^{2^n} + 1$$
$$f_0 = 2^1 + 1 = 3$$
$$f_1 = 2^2 + 1 = 5$$
$$f_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$
$$f_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$
$$f_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$$
$$f_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

Ok, clearly I can see the pattern

$$3+2=5$$

$$(3)(5)+2=17$$

$$(3)(5)(17)+2=257$$

So from this limited data the recursion is true. But why does the recursion hold true for all n? Let's try to make sense of why this works.

Look at this here table

Index n	0	1	2	3	4	5	6	7
Value 2^n	1	2	4	8	16	32	64	128

n determines the power of 2 on 2. Example 2^{2^n}.

Gathering some data on 2^{2^n}

$$2^{2^n}$$

$$2^{2^0}=2^1=2$$

$$2^{2^1}=2^2=4$$

$$2^{2^2}=2^4=16$$

$$2^{2^3}=2^8=256$$

$$2^{2^4}=2^{16}=65536$$

$$2^{2^5}=2^{32}=4294967296$$

Alright, so adding 1 gives us the Fermat Numbers. I assume he added 1 to make the number odd. I also assume he picked, 2^{2^n} as it follows the general trend of prime numbers.

Gathering some data about the proposed recurrence.

$$f_0-2=1$$

$$f_1-2=(2^{2^0}+1)=(2^1+1)=(3)=3$$

$$f_2-2=(2^{2^0}+1)(2^{2^1}+1)=(2^1+1)(2^2+1)=(3)(5)=15$$

$$f_3-2=(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)=(2^1+1)(2^2+1)(2^4+1)=(3)(5)(17)=255$$

$$f_4-2=(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)(2^{2^3}+1)=(2^1+1)(2^2+1)(2^4+1)(2^8+1)=(3)(5)(17)(257)=65535$$

$$f_4-2=(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)(2^{2^3}+1)(2^{2^4}+1)=(3)(5)(17)(257)(65537)=4294967295$$

Why do you always have to add 2 to get to the Fermat Number?

$$5-2=2^1+1$$

$$17-2=(2^1+1)(2^2+1)$$

$$17-2=2^1*2^2+2^1+2^2+1$$

$$17-2=2^{1+2}+2^1+2^2+1$$

$$17-2=2^3+2^1+2^2+1$$

$$17 - 2 = 2^3 + 2^2 + 2^1 + 1$$

$$257 - 2 = (2^1 + 1)(2^2 + 1)(2^4 + 1)$$
$$257 - 2 = (2^3 + 2^2 + 2^1 + 1)(2^4 + 1)$$
$$257 - 2 = 2^3 * 2^4 + 2^3 + 2^2 * 2^4 + 2^2 + 2^1 * 2^4 + 2^1 + 2^4 + 1$$
$$257 - 2 = 2^{3+4} + 2^3 + 2^{2+4} + 2^2 + 2^{1+4} + 2^1 + 2^4 + 1$$
$$257 - 2 = 2^7 + 2^3 + 2^6 + 2^2 + 2^5 + 2^1 + 2^4 + 1$$
$$257 - 2 = 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 1$$

Alright, clearly a summation is at work.

Let $N = 2^n$

$$f_n = 2^N + 1 = (\sum_{k=0}^{N-1} 2^k) + 2 = f_0 \cdot f_1 \cdot f_2 \cdots f_{n-1} + 2$$

3. Compute $199^{65571} \mod 193$. Do as much of this as possible with your brain, and show your work.

Fact 1

$$a^{p-1} \equiv 1 \mod p$$

$$199^{65571} \mod 193$$

mod the 199

$$6^{65571} \mod 193$$

192 goes into 65571 $\rightarrow$ 341 with a remainder of 99

$$6^{(192)(341)+99} \mod 193$$

I can get rid of 192 in the exponent because of Fact 1

$$6^{99} \mod 193$$

$6 * 6 * 6 \mod 193$ is 23 and we are doing that 33 times

$$23^{33} \mod 193$$

$$23^{32} * 23 \mod 193$$

I did the last bit with a calculator but $23^{32} \mod 193$ is 1

$$23 \mod 193$$

4. Find the smallest positive integer x such that

$$x \equiv 11 \mod 24, \text{ and}$$
$$x \equiv 16 \mod 35.$$

$$x = 16 + 35q$$
$$x = 11 + 24k$$

Subtract equations

$$0 = 5 + 35q + 24(-k)$$
$$-5 = 35q + 24(-k)$$
$$5 = 35(-q) + 24k$$

Do the shifty-shifty algorithm.

$$35 = 24(1) + 11 -> 11 = -24(1) + 35$$
$$24 = 11(2) + 2 -> 2 = -11(2) + 24$$
$$11 = 2(5) + 1 -> 1 = -2(5) + 11$$

Do the continuation-of-the-shifty-shifty algorithm.

$$1 = -2(5) + 11$$

Plug in $-11(2) + 24$ for 2

$$1 = -(-11(2) + 24)(5) + 11$$
$$1 = 11(10) - 24(5) + 11$$
$$1 = 11(11) - 24(5)$$

Plug in $-24(1) + 35$ for 11

$$1 = (-24(1) + 35)(11) - 24(5)$$
$$1 = -24(11) + 35(11) - 24(5)$$
$$1 = -24(16) + 35(11)$$

Now I need to multiply both sides by 5 to make it look like the third equation from the top.

$$5 = 24(-16)(5) + 35(11)(5)$$

$$5 = 35(11)(5) + 24(-16)(5)$$
$$5 = 35(-q) + 24k$$

Alright so

$$-q = (11)(5)$$
$$q = (-11)(5)$$
$$k = (-16)(5)$$

Plugging into the originals

$$x = 16 + 35q$$

$$x = 16 + 35(-11)(5)$$
$$x = -1909$$

But remember this is being modded by 840

$$x = 611$$

$$x = 11 + 24k$$
$$x = 11 + 24(-16)(5)$$
$$x = -1909$$

Alright so let's check the work

$$611 \mod 35 = 16$$
$$611 \mod 24 = 11$$

Well, that looks right to me!

5. Determine (and display) the prime factorization of 50!. (Note that the sentence is not an exclamation! You're asked to find the prime factorization of 50-factorial.)

   How many numbers from [1..50] are divisible by 2? Well 25, all the even numbers. How about 4? Well 12, it's half of the even numbers are also divisible by 4.

   Here is table displaying this information

n	n	n^2	n^3	n^4	n^5
2	25	12	6	3	1
3	18	5	1		
5	10	2			
7	7	1			
11	4				
13	3				
17	2				
19	2				
23	2				
29	1				
31	1				
37	1				
41	1				
43	1				
47	1				

   So the prime factorization of 50! is

$$50! = 2^{25+12+6+3+1} * 3^{18+5+1} * 5^{10+2} * 7^{7+1} * 11^4 * 13^3 * 17^2 * 19^2 * 23^2 * 29^1 * 31^1 * 37^1 * 41^1 * 43^1 * 47^1$$