**MATH 4410**
**Nate Stott A02386053**

---

**Quiz #10; Due 11:59 pm, 4/10/2024**

1. Decrypt the message sent over Canvas using public key $(e, n) = (253, 899)$. Here's the message again (remember it has been broken into blocks/chunks of three letters any of which could be a space):

   412 596 692 52 244 121 343 761 121

   START

   $$(e, n) = (253, 899)$$

   I used my python program to give me d

   $$d = 757$$

   decrypt:

   $$(m^e)^d \equiv m^d \mod n$$

   $$m = 412$$

   $$(412^{253})^{757} \equiv 412^{757} \mod 899$$

   Calculator for all
   $412 \to 847$
   $596 \to 741$
   $692 \to 547$
   $52 \to 197$
   $244 \to 418$
   $121 \to 324$
   $343 \to 314$
   $761 \to 384$
   $121 \to 324$

From another program I made:
'I', 'S'
'E', 'O', 'Y'
'H', 'R'
'H', 'R'
'E', 'O', 'Y'
'B', 'L', 'V', ' '
'F', 'P', 'Z'
'E', 'O', 'Y'
'H', 'R'
'B', 'L', 'V', ' '
'J', 'T'
'H', 'R'
'E', 'O', 'Y'
'B', 'L', 'V', ' '
'I', 'S'
'D', 'N', 'X'
'C', 'M', 'W'
'E', 'O', 'Y'
'D', 'N', 'X'
'B', 'L', 'V', ' '
'E', 'O', 'Y'
'D', 'N', 'X'
'I', 'S'
'E', 'O', 'Y'
'D', 'N', 'X'
'C', 'M', 'W'
'E', 'O', 'Y'

I saw the "sorry for the " part pretty quickly

I had to get help from a friend to see the next part, I didn't realize how long "inconvenience" is hahah

Decrypted message: "sorry for the inconvenience"

END

2. Consider all binary strings of length $n$ (a.k.a. sequences consisting of 0s and 1s of length $n$). Define a **prime binary string** to be a binary string that is *not* expressible as the concatenation of several identical smaller binary strings. For example, 100100100 is not prime, but 1101 is a prime binary string.

   (a) Determine a formula (should be a divisor sum) for the number $f(n)$ of prime binary strings of length $n$.

   START

   Let $m$ be the Möbius function

   $f(n) = 2^n - \sum_{d|n} f(d)$ where d is not equal to n

$$f(n) + \sum_{d|n} f(d) = 2^n$$

   By MIT

$$f(n) = \sum_{d|n} 2^d * m(\frac{n}{d})$$

   END

(b) For $n$ ranging over some substantial interval (should be at least [1..20]), compute $f(n)$ and conjecture an approximate elementary* function for $f(n)$, or for the ratio $f(n)/2^n$.

START

$g(n) = 2^n - 2^{gd(n)}$ where $gd(n)$ is defined as the greatest divisor of $n$ but not including $n$.

$$f(n) = \sum_{d|n} 2^d * m(\frac{n}{d})$$

*The term '*elementary*' when said of a function means the function is a single-variable function that is expressible as a finite number of sums, products, roots or compositions of polynomial, rational, trigonometric, hyperbolic, and exponential functions – the ones you torture in Calculus.

$$g(1) = 0$$
$$f(1) = 2$$

$$f(2) = 2$$
$$f(2) = 2$$

$$g(3) = 6$$
$$f(3) = 6$$

$$g(4) = 14$$
$$f(4) = 12$$

$$g(5) = 30$$
$$f(5) = 30$$

$$f(6) = 62$$
$$f(6) = 54$$

$$g(7) = 126$$
$$f(7) = 126$$

$$g(8) = 254$$
$$f(8) = 240$$

$$g(9) = 510$$
$$f(9) = 504$$

$$g(10) = 1022$$
$$f(10) = 990$$

$$g(11) = 2046$$
$$f(11) = 2046$$

$$f(12) = 4094$$
$$f(12) = 4020$$

$$g(13) = 8190$$
$$f(13) = 8190$$

$$g(14) = 16382$$
$$f(14) = 16254$$

$$g(15) = 32766$$
$$f(15) = 32730$$

$$g(16) = 65534$$
$$f(16) = 65280$$

$$g(17) = 131070$$
$$f(17) = 131070$$

$$g(18) = 262142$$
$$f(18) = 261576$$

$$g(19) = 524286$$
$$f(19) = 524286$$

$$g(20) = 1048574$$
$$f(20) = 1047540$$

It appears that when $n$ is even the approximation is spot on.

END

3. A long-ass time ago Euclid published a proof of the following statement in Book IX of *The Elements*:

> If as many numbers as we please beginning from a unit are set out continuously in double proportion until the sum of all becomes prime, and if the sum multiplied into the last makes some number, then the product is perfect.

In other terms, the ones we use, *If* $(1+2+4+8+\cdots+2^{n-1})$ *is prime, then* $(2^n-1)2^{n-1}$ *is perfect.* Note that, as any CAPOTS [†] knows, $1+2+4+\cdots+2^{n-1} = 2^n-1$. Also, if $2^n-1$ is prime, then $n$ must be prime. A perfect number N is thus said to be *of Euclid type* if $N = (2^p-1)2^{p-1}$, where $p$ and $2^p-1$ are prime. We'll prove both these facts in class; what I'd like you to prove is this:

*If* $n$ *is an even perfect number, then* $n$ *is of Euclid type; that is,* $n = (2^p-1)2^{p-1}$*, where* $2^p-1$*, is prime.*

Euler proved this about 2000 years after Euclid wrote and published the elements; it is the closest result to a characterization of perfect numbers that I know of. It does not rule out the possibility of the existence of odd perfect numbers.

START

Let $o(n) = 2n$ where $o$ is the sum of the divisors function we talked about in class

Prove: $n = (2^p-1)2^{p-1}$, where $2^p-1$, is prime.

$n = x * 2^{k-1}$ where $(x = 2w-1)$

I know that $x$ is relatively prime to $2^{k-1}$ because $x$ is odd and $2^{k-1}$ is a multiple of 2.

Thus $o(x * 2^{k-1}) = o(x) * o(2^{k-1})$

by the geometric series formula $o(x * 2^k - 1) = o(x) * 2^k - 1$

therefore $x * 2^k = o(x)2^k - 1$

$$o(x) = \frac{x * 2^k}{2^k - 1}$$

[†] Common attentive person on the street.

I know that $o(x)$ has to be an integer. So $2^k - 1$ has to divide either $x$ or $2^k$. I know that $2^k$ is even and $2^k - 1$ is odd, so $2^k - 1$ has to divide $x$.

$$2^k - 1 | x$$
$$x = (2^k - 1)u$$

So I need to prove that $u$ has to be 1. Let's do this by contradiction.

Assume $x$ is not prime.

Where $p$ is prime.

$$x = p_1^{e_1} p_2^{e_2} p_3^{e_3} ... p_i^{e_i}$$

$$o(x) = o(p_1^{e_1}) o(p_2^{e_2}) o(p_3^{e_3}) ... o(p_i^{e_i})$$

by the geometric series formula

$$o(x) = (\frac{p_1^{e_1+1} - 1}{p_1 - 1})(\frac{p_2^{e_2+1} - 1}{p_2 - 1})(\frac{p_3^{e_3+1} - 1}{p_3 - 1})...(\frac{p_i^{e_i+1} - 1}{p_i - 1})$$

R is an unsure relationship $=, <, >$.

$$2^k p_1^{e_1} p_2^{e_2} p_3^{e_3} ... p_i^{e_i} R(\frac{p_1^{e_1+1} - 1}{p_1 - 1})(\frac{p_2^{e_2+1} - 1}{p_2 - 1})(\frac{p_3^{e_3+1} - 1}{p_3 - 1})...(\frac{p_i^{e_i+1} - 1}{p_i - 1})(2^k - 1)$$

Simplifying

$$2^k (p_1^{e_1+1} - p_1)(p_2^{e_2+1} - p_2)(p_3^{e_3+1} - p_3)...(p_i^{e_i+1} - p_i) R (p_1^{e_1+1} - 1)(p_2^{e_2+1} - 1)(p_3^{e_3+1} - 1)...(p_i^{e_i+1} - 1)(2^k - 1)$$

Clearly the left side is smaller than the right side as you are subtracting a whole copy rather than one.

This means that $x$ has to be prime.

Which means that $u$ has to be 1

Eurkia! It is proved. $n = (2^p - 1)2^{p-1}$, where $2^p - 1$, is prime.

END