MATH310 Homework 10

Chris Camano: ccamano@sfsu.edu

November 14, 2022

Stein 1.13

1. Prove that if a postive integer n is a perfect square, then n cannot be written in the form 4k+4 for k an integer.
2. Prove that no integers in the sequence:

$$11, 111, 1111, \cdots$$

is a perfect square

Proof. if n is of the form: $4k+3$ we can show that n must then be odd since :

$$4k+3 = 2(2k+1)+1$$

so if there exists a value x such that $x^2 = 4k+3$ then we can show by the definition of an odd number for an odd number of the form : $(2l+1)$that :

$$\begin{aligned}
(2l+1)^2 &= 4k+3 \\
4l^2+4l+1 &= 4k+3 \\
4l^2+4l-4k+1 &= 3 \\
4(l^2+l-k)+1 &= 3 \\
4(l^2+l-k) &= 2 \\
2(l^2+l-k) &= 1 \\
(l^2+l-k) &= \frac{1}{2}
\end{aligned}$$

which is a contradiction since k and l are integers . □

Since numbers of the form 111... have remainder 3 mod 4 it can be shown that by the first proof since numbers of the form 4k+3 are never perfect squares that the sequence contains no perfect squares.
Below is the proof : let the elements of the sequence be generated by the following expression:

$$a_n = \sum_{i=0}^{n} 10^i$$

Since 4 divides all values of this sequence for $i > 2$ we can consider the following:

$$\sum_{i=0}^{n} 10^i = 11 + \sum_{i=2}^{n} \equiv 11 \mod 4$$

Which is the same as :

$$11 \equiv 3 \mod 4$$

and by the proof of part a we know that numbers of the forma 4k+3 cannot be perfect squares Thus we conclude that no elements of the sequence are perfect sqaures.

Andrews 5.1.3

Find $\tilde{a}$, the inverse of a modulo c, when :

1. $a = 2$ and $c = 5$
2. $a = 7$ and $c = 9$
3. $a = 12$ and $c = 17$

Proof. Since the values of a and c are relatively small most of these were computed by inspection, we Know that there exists an inverse if a and c are coprime and in this case all a and c are in fact coprime meaning its worthwhile to consider potential solutions.

1. $a = 2$ and $c = 5$
   The modular inverse of a is 3 since:
   $$6 \equiv 1 \mod 5$$
2. $a = 7$ and $c = 9$
   The modular inverse of a is 4 since:
   $$28 \equiv 1 \mod 9$$
3. $a = 12$ and $c = 17$

   The modular inverse of a is 10 since:
   $$120 \equiv 1 \mod 17$$

□

Andrews 5.2.5

What is the remainder when 41^{75} is divided by 3?

Proof. Using Fermat's little theorem we know that:

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

in our context:

$$n^2 \equiv 1 \mod 3$$

Leveraging this fact we can re-express our original problem as follows:

$$
\begin{aligned}
&41^{75} \equiv x \mod 3 \\
&41(41^{37})^2 \equiv x \mod 3 \\
&41 \equiv x \mod 3 \\
&41^{75} \equiv 41 \equiv 2 \mod 3
\end{aligned}
$$

□

Andrews 5.2.6

What is the remainder when 473^{38} is divided by 5?

Proof. Again Using Fermat's little theorem we know that:

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

in our context:

$$n^4 \equiv 1 \mod 5$$

Leveraging this fact we can re-express our original problem as follows:

$$
\begin{aligned}
&473^{38} \equiv x \mod 5 \\
&473^2(473^4)^9 \equiv x \mod 5 \\
&473^2 \equiv x \mod 5
\end{aligned}
$$

473^2 is a fairly large number but luckily since we are working mod 5 we only need to consider the final digit since the rest will be divisible by 5. giving:

$$473^{38} \equiv 473^2 \equiv 3^2 \equiv 9 \equiv 4 \mod 5$$

□

Problem 5

If n is composite then $2^n - 1$ is composite. Compute using computational methods 3 numbers of the form $2^n - 1$ that are prime

Proof. Let n be composite, then n-= kp where p is a prime

$$2^n - 1 = 2^{kp} - 1$$

$$(2^k)^p - 1$$

$$\frac{(2^k)^p - 1}{2^k - 1}(2^k - 1)$$

Note that this is the result of a finite geometric series:

$$\left[\sum_{i=1}^{p} (2^k)^{p-i}\right](2^k - 1)$$

Both of these are integers so we have shown that $2^n - 1$ is a composite number since it is the produc tof two integers

$\square$

Proof. Numbers of the form $2^n - 1$ that are prime are denoted Mersenne primes. The converse of the contrapositive of the statement above is also true meaning that if n is prime then $2^n - 1$ is prime as well. So to generate 3 numbers of this form we can simply pick the first 3 primes and observe the results

$$\begin{aligned} n = 2 \quad &: 2^2 - 1 = 3 \\ n = 3 \quad &: 2^3 - 1 = 7 \\ n = 5 \quad &: 2^5 - 1 = 31 \end{aligned}$$

$\square$