MATH 310 Homework 9?

Chris Camano: ccamano@sfsu.edu

October 31, 2022

Question 1:Andrews 3.2.2

Prove that if $12|n^2-1$ if gcd(n,6)=1

Proof. We first remind ourselves of Fermat's little theorem:

$$\text{If p is a prime and n is an integer then } p|p^2-n$$

If $12|n^2-1$, then by definition of divisibility we know that:

$$n^2-1=12k, k \in \mathbb{Z}$$

So we wish to show that n^2-1 is a multiple of 12.
We now leverage the gcd statment given to us to combine with this observation: If n and 6 are coprime then this implies that n is 1 less or more than a multiple of 6 six since 6 is not relativley prime to integers 2,3,4 but is for 5 and 7 .

Using this fact we know that in general n is going to assume the form:

$$6l+1, \text{ or } 6l-1 \rightarrow 6l \pm 1, l \in \mathbb{Z}$$

$$\begin{aligned}
&(6l \pm 1)^2-1 \\
&36l^2 \pm 12l+1-1 \\
&12(3l^2 \pm l) \\
&\therefore 12|n^2-1
\end{aligned}$$

If I was really feeling it I would split this in cases instead of preserving the plus minus sign but Ill let you fill in the blanks ☐

Question 2: Andrews 4.1.2

Do there exist integers x such that

1. $6x \equiv 5 (\mod 4)$

2. $10x \equiv 8 (\mod 6)$

3. $12x \equiv 9 (\mod 6)$

Proof.

1. gcd(6,4)=2 however note that : $4 \nmid 5$ so by theorem 5-1 there are no solutions
2. gcd(10,6)=2, $2|8$ so there are 4 unique solutions to this congruence by theorem 5-1
3. gcd(12,6)=6, $6 \nmid 9$ so there are no solutions to this congruence by theorem 5-1.

□

Question 3: Andrews 7.1.6

Find all primitive roots modulo 5, modulo 9, modulo 11, modulo 13, and modulo 15

Proof.

1. 5
   We start by computing $\phi(5) = 4$ so the question stands: Does there exist an a$\in \mathbb{Z}_5$ such that $a^n \equiv 1$ mod $5, n < \phi(5)$? Here 5 is coprime to the elements of $\mathbb{Z}_5$ so we need to consider all elements.
   By theorem 7-5 there should be $\phi(\phi(5)) = 2$ primitive roots.

   The two primite roots of 5 are : 2 and 3
2. 9
   By theorem 7-5 there should be $\phi(\phi(9)) = 2$ primitive roots

   The two primitive roots of 9 are: 2,5
3. 11
   By theorem 7-5 there should be $\phi(\phi(11)) = 4$ primitive roots

   The four primitive roots of 11 are :2,6,7,8
4. 13
   By theorem 7-5 there should be $\phi(\phi(13)) = 4$ primitive roots

   The four primitive roots of 13 are : 2,6,7,11
5. 15
   15 does not have primitive roots, evaluating the reduced residue system: $\phi(15) = 8$

$$
\begin{aligned}
2^4 &\mod 15 = 1\\
4^2 &\mod 15 = 1\\
7^4 &\mod 15 = 1\\
8^4 &\mod 15 = 1\\
11^2 &\mod 15 = 1\\
13^4 &\mod 15 = 1\\
14^2 &\mod 15 = 1
\end{aligned}
$$

$\square$

Code I wrote to generate solutions (c++):

```
int gcd(int a, int b)
{
        if (a == 0)
                return b;
        return gcd(b % a, a);
}
int phi(int n) {
        unsigned int result = 1;
        for (int i = 2; i < n; i++)
                if (gcd(i, n) == 1)
                        result++;
        return result;
}
void findPrimitiveRoots(int n) {
        cout << "________Primitive_Root_Finder________" << endl;
        vector<int> rrs;
        for (int i = 2; i < n; i++) {
                if (gcd(i, n) == 1) {
                        rrs.push_back(i);
                }
        }

        for (int i = 0; i < rrs.size(); i++) {
                bool is_not_root = false;
                for (int j = 2; j < phi(n); j++) {
                        if (int(pow(rrs[i], j)) % n == 1) {
                                is_not_root = true;
                                double b = pow(rrs[i], j);
                                cout << endl;

                                cout << rrs[i] << "_is_not_a_primitive_root_" << endl;

                                cout << "Remainder_" << (int(b)) % n << "_for_" <<
                      rrs[i] << "^" << j << endl;
                                cout << pow(rrs[i], j) << "_mod_" << n << "=" <<
                      (int(b)) % n << endl;

                                break;
```

```
			}
		}
		if (!is_not_root) {
			cout << endl;

			cout << rrs[i] << " is a primitive root" << endl;

		}
	}
}
```

Question 4: Andrews 7.2.15

How many primitive roots exist for the moduli 6,7,8,9,10?

Proof.

1.
$$\begin{aligned}&\phi(\phi(6))\\&\phi(2)=1\end{aligned}$$

   So by theorem 7-5 there is 1 primitive root

2.
$$\begin{aligned}&\phi(\phi(7))\\&\phi(6)=2\end{aligned}$$

   So by theorem 7-5 there are 2 primitive roots

3. 8 has no primitive roots proof below
$$\begin{aligned}3^2 &\equiv 1 \mod 8\\5^2 &\equiv 1 \mod 8\\7^2 &\equiv 1 \mod 8\end{aligned}$$

4.
$$\begin{aligned}&\phi(\phi(9))\\&\phi(6)=2\end{aligned}$$

   So by theorem 7-5 there are 2 primitive roots

5.
$$\begin{aligned}&\phi(\phi(10))\\&\phi(4)=2\end{aligned}$$

   So by theorem 7-5 there 2 primitive roots

□

Question 5: Stein 2.23

Find all four solutions to the equation :

$$x^2 - 1 \equiv 0 \mod 35$$

$$x^2 \equiv 1 \mod 35$$

Solutions: 1,6,29,34

Proof. **proof by being a computer scientist**

Code I wrote to generate solutions (c++):

```
for (int i = 1; i < 35; i++) {
                        if (int(pow(i, 2)) % 35 == 1) {
                                cout << i << " is a solution " << endl;
                        }
        }
```

□

A more "theoretic" proof:

Proof. We can start by splitting congruence as follows:

$$x^2 \equiv 1 \mod 5$$
$$x^2 \equiv 1 \mod 7$$

if remove the sqaure root we end up generating four sub problems which luckily alligns with out problem description:

$$x \equiv 1 \mod 7$$
$$x \equiv 1 \mod 5$$

Here we see very clearly that the solution to this system is just 1

$$x \equiv -1 \mod 7 \rightarrow x \equiv 6 \mod 7$$
$$x \equiv -1 \mod 5 \rightarrow x \equiv 4 \mod 5$$

Here we see the solution of 34

$$x \equiv -1 \mod 7 \rightarrow x \equiv 6 \mod 7$$
$$x \equiv 1 \mod 5$$

Next we can see by inspection the solution of 6

$$x \equiv 1 \mod 7$$
$$x \equiv -1 \mod 5 \rightarrow x \equiv 4 \mod 5$$

finally our last solution is 29 □