Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

1.26

Let {p1, p2,...,pr} be a set of prime numbers, and let N = p1p2 ··· pr + 1

1. The first step is let q be a value that can divide N, and suppose it is one of the p's in the equation.
2. Now if we rearrange the equations we would have 1 = N – p1p2….pr ≡ 0 (mod q)
3. Since q would be able to divide both N and p1p2…pr we would be left with q | 1, which is not possible. Which proves that q can't be equal to any of the p's.
4. Next we will assume there are a finite number of primes. Meaning we could list every prime in our list p1p2…pr.
5. However, our equation produces a new prime number every time that is not in our list which would contradict the assumption that there is a finite amount of prime numbers, meaning there are infinitely many.

1.31

a) Using Fermat's Little Theorem/Proposition 1.30, given

$a \in \mathbb{F}_p^*$ and $b = a^{(p-1)/q}$,

when we raise both sides of the equation by q we get,

$b^q \equiv a^{\overline{\frac{p-1}{q}}^{q}} \equiv 1\ (mod\ p)$ or

$b^q \equiv q^{p-1} \equiv 1\ (mod\ p)$.

So, the order of b divides the prime q and if $b \neq 1$, then b has order q by the theorem.

b) Using the Primitive Root Theorem/Theorem 1.31, let g and p be primitive roots. Let

$a \equiv g^k\ (mod\ p)$.

Then,

$g^{k^{(p-1)/q}} \equiv 1\ (mod\ p)$ if and only if $p - 1$ divides $k(p - 1)/q$ given by part a.

That is, if and only if k is a multiple of q.

There are $(p - 1)/q$ such multiples of q in the interval 0 to $p - 1$. Thus, the probability of $a^{(p-1)/q} \equiv 1$ is $\frac{(p-1)/q}{(p-1)}$ or $\frac{1}{q}$. So, the probability of success is $1 - \frac{1}{q}$ to find

$b = a^{(p-1)/q}$ such that $b \neq 1$.

Problem 1.32

a) For which of the following primes is 2 a primitive root modulo p?

Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

i) $p = 7$

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 1; 2^4 = 2; 2^5 = 4;

Answer: NO

ii) $p = 13$

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 3; 2^5 = 6; 2^6 = 12; 2^7 = 11; 2^8 = 9;

2^9 = 5; 2^10 = 10; 2^11 = 7;

Answer: YES

iii) $p = 19$

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 =13; 2^6 = 7; 2^7 = 14; 2^8 = 9;

2^9 = 18; 2^10 = 17; 2^11 = 15; 2^12 = 11; 2^13 = 3; 2^14 = 6; 2^15 = 12;

2^16 = 5; 2^17 = 10;

Answer: YES

iv) $p = 23$

2^0 = 1; 2^1 = 2; 2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 = 9; 2^6 = 18; 2^7 = 13; 2^8 = 3;

2^9 = 6; 2^10 = 12; 2^11 = 1; 2^12 = 2; 2^13 = 4; 2^14 = 8; 2^15 = 16;

2^16 = 9; 2^17 = 18; 2^18 = 13; 2^19 = 3; 2^20 = 6; 2^21 = 12;

Answer: NO

b) For which of the following primes is 3 a primitive root modulo p?

i) $p = 5$

3^0 = 1; 3^1 = 3; 3^2 = 4; 3^3 = 2;

Answer: YES

ii) $p = 7$

3^0 = 1; 3^1 = 3; 3^2 = 2; 3^3 = 6; 3^4 = 4; 3^5 = 5;

Answer: YES

iii) $p = 11$

3^0 = 1; 3^1 = 3; 3^2 = 9; 3^3 = 5; 3^4 = 4; 3^5 = 1; 3^6 = 3; 3^7 = 9; 3^8 = 5;

Answer: NO

Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

iv) $p = 17$

$3^0 = 1$; $3^1 = 3$; $3^2 = 9$; $3^3 = 10$; $3^4 = 13$; $3^5 = 5$; $3^6 = 15$; $3^7 = 11$;

$3^8 = 16$; $3^9 = 14$; $3^{10} = 8$; $3^{11} = 7$; $3^{12} = 4$; $3^{13} = 12$; $3^{14} = 2$; $3^{15} = 6$;

Answer: YES

c) Find a primitive root for each of the following primes.

i) $p = 23$

Answer: 2 is a primitive root.

Explanation: $2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 16$; $2^5 = 9$; $2^6 = 18$;

$2^7 = 13$; $2^8 = 3$; $2^9 = 6$; $2^{10} = 12$; $2^{11} = 1$; $2^{12} = 2$; $2^{13} = 4$;

$2^{14} = 8$; $2^{15} = 16$; $2^{16} = 9$; $2^{17} = 18$; $2^{18} = 13$; $2^{19} = 3$; $2^{20} = 6$;

$2^{21} = 12$;

ii) $p = 29$

Answer: 2 is a primitive root.

Explanation: $2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 16$; $2^5 = 3$; $2^6 = 6$;

$2^7 = 12$; $2^8 = 24$; $2^9 = 19$; $2^{10} = 9$; $2^{11} =18$; $2^{12} = 7$; $2^{13} = 14$;

$2^{14} = 28$; $2^{15} = 27$; $2^{16} = 25$; $2^{17} = 21$; $2^{18} = 13$; $2^{19} = 26$; $2^{20} = 23$;

$2^{21} = 17$; $2^{22} = 5$; $2^{23} = 10$; $2^{24} = 20$; $2^{25} = 11$; $2^{26} = 22$; $2^{27} = 15$;

iii) $p = 41$

Answer: 6 is a primitive root

Explanation: $6^0 = 1$; $6^1 = 6$; $6^2 = 36$; $6^3 = 11$; $6^4 = 25$; $6^5 = 27$; $6^6 = 39$;

$6^7 = 29$; $6^8 = 10$; $6^9 = 19$; $6^{10} = 32$; $6^{11} = 28$; $6^{12} = 4$; $6^{13} = 24$;

$6^{14} = 21$; $6^{15} = 3$; $6^{16} = 18$; $6^{17} = 26$; $6^{18} = 33$; $6^{19} = 34$; $6^{20} = 40$;

$6^{21} = 35$; $6^{22} = 5$; $6^{23} = 30$; $6^{24} = 16$; $6^{25} = 14$; $6^{26} = 2$; $6^{27} = 12$;

$6^{28} = 31$; $6^{29} = 22$; $6^{30} = 9$; $6^{31} = 13$; $6^{32} = 37$; $6^{33} = 17$; $6^{34} = 20$;

$6^{35} = 38$; $6^{36} = 23$; $6^{37} = 15$; $6^{38} = 8$; $6^{39} = 7$;

(e) Write a computer program to check for primitive roots and use it to find all primitive roots modulo 229. Verify that there are exactly ϕ229 of them.

Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

Program is on GitHub, “Crypt_hw2_E.java”

6, 7, 10, 23, 24, 28, 29, 31, 35, 38, 39, 40, 41, 47, 50, 59, 63, 65, 66, 67, 69, 72, 73, 74, 77, 79, 87, 90, 92, 96, 98, 102, 105, 110, 112, 113, 116, 117, 119, 124, 127, 131, 133, 137, 139, 142, 150, 152, 155, 156, 157, 160, 162, 163, 164, 166, 170, 179, 182, 188, 189, 190, 191, 194, 198, 200, 201, 205, 206, 219, 222, 223

ϕ229 = 72, program returned 72 primitive roots

(f) Use your program from (e) to find all primes less than 100 for which 2 is a primitive root.

3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83

(g) Repeat the previous exercise to find all primes less than 100 for which 3 is a primitive root. Ditto to find the primes for which 4 is a primitive root.

Primes with 3 as a primitive root:

5, 7, 17, 19, 29, 31, 43, 53, 79, 89

Primes with 4 as a primitive root:

There are no primes less than 100 for which 4 is a primitive root

1.33

Since $g \not\equiv 1 \; mod \; p$, $g^q \not\equiv 1 \; mod \; p$, and q is prime, this shows that p-1 is the largest exponent such that $g^{p-1} \equiv 1 \; mod \; p$. This is shown to be true in Proposition 1.30. Since p-1 is the largest exponent, we can conclude that for the rest of the exponent g^0 to g^{p-2} that they give every element of $\mathbb{F}_p^*$. This can be shown when p = 7, g = 3, and q = 3.

1.34

a)

- Lets assume x is a square root mod p. If $x^2 = b$ (mod p) is true then we can assume that there is another solution, -x. So $-x^2 = b$ (mod p) ≡ $x^2 = b$ (mod p)
  To prove there are only two solutions lets assume that there is some number y that y ≠ x (mod p) and y ≠ -x (mod p) but $y^2 = b$ (mod p). So $x^2 = b = y^2$ which is $x^2 – y^2 = b - b \equiv (x – y)(x + y)$. Possible integers are p / (x – y)(a + y).
  Using p / (x – y) , where y = a(mod p) this contradicts the assumption that y≠ x (mod p).
  Therefore, b must have exactly 2 solutions if it has one solution.
- If p = 2 then the only possible ways to obtain solutions is if b is a 1
- If p/b then there are no square roots mod p

b)

i) (p,b) = (7,2) $x^2 = 2$ (mod 7)

Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

0 1 2 **3** **4** 5 6 7 8 9 **10** **11** 12 13 14 15 16 **17** **18** (squared and modulo 7)

0 1 4 2 2 4 1 0 1 4 2 2 4 1 0 1 4 2 2

There seems to be a pattern. Any integer mod 7 that equals 3 or 4 is a solution

And taking the negative of that number and doing modulo 7 they will result in either a 3 or 4 those are solutions as well.

Examples: -3 mod 7 = 4 -11 mod 7 = 3

ii) (p,b) = (11,5) x^2 = 5 (mod 11)

0 1 2 3 **4** 5 6 **7** 8 9 10 11 12 13 14 **15** 16 17 **18** (squared and modulo 11)

0 1 4 9 5 3 3 5 9 4 1 0 1 4 9 5 3 3 5

Solutions can be found when, x mod 11 = 4 or x mod 11 =7

iii) (p,b) = (11,7) x^2 = 7 (mod 11)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 (squared and modulo 11)

No solutions

iv) (p,b) = (7,2) x^2 = 3 (mod 37)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 **15** 16 17 18 (squared and modulo 37)

0 1 3 9 16 25 1 12 27 7 26 10 33 21 11 3 34 30 28

Solutions are 15 and – 15

c) how many square roots does 29 have modulo 35? Why doesn't this contradict the assertion (a) ?

0 1 2 3 4 5 6 7 **8** 9 10 11 12 13 14 15 16 17 18 x^2 = 29 (mod 35)

0 1 4 9 16 25 1 14 29 11 30 16 4 29 21 15 11 9 9 11 15 21 29

8 and -8 are square roots. It doesn't contradict because it is either 2 solutions or no solutions.

d) Let p be an odd prime and let g be a primitive root modulo p. Then any number a is equal to some power of g modulo p, say a ≡ g^k (mod p). Prove that a has a square root modulo p if and only if k is even.

Let's assume k is even. Then k = 2n (k being divisible by 2), so a a ≡ g^{2n} (mod p).

1.36

Group 2: Kyle, Jesus, Ying, Mason, Gage, Adam, Connor

Compute the value of

$2(p-1)/2 \pmod p$

for every prime $3 \leq p<20$. Make a conjecture as to the possible values of $2(p-1)/2 \pmod p$ when p is prime and prove that your conjecture is correct.

Ans:

My conjecture is for the prime number 3, 5, 7 the possible value is 2 ,4 ,1 respectively and it will be repeat showing it.

The program proves my conjecture.

The value of prime number 3 is: 2

The value of prime number 5 is: 4

The value of prime number 7 is: 1

The value of prime number 9 is: 2

The value of prime number 11 is: 4

The value of prime number 13 is: 1

The value of prime number 15 is: 2

The value of prime number 17 is: 4

The value of prime number 19 is: 1