18.781
PROBLEM SET3

JOHN WANG

1. Problem 1

Problem 1.1. *Solve the congruence* $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.

Solution First, we note that the prime factorization of $143 = (11)(13)$. Thus, we can take the congruence modulo 11 and 13 to create two new congruences, since 11 and 13 are prime. This yields:

$$x^3 + 2x^2 + x + 7 \equiv 0 \pmod{11} \tag{1.1}$$
$$x^3 + 4x^2 + 10x + 11 \equiv 0 \pmod{13} \tag{1.2}$$

In the first equation, we can check all $x \in \{0, 1, \ldots, 10\}$, and we find that the congruence holds for $x = 1, 3, 5$. We can do the same in the second equation, and we see that the congruence also holds for $x = 1, 3, 5$. Thus, we want to find solutions to the simultaneous equations $x \equiv a \pmod{11}$ and $x \equiv b \pmod{13}$ where $a \in \{1, 3, 5\}$ and $b \in \{1, 3, 5\}$. Now we can use the Chinese Remainder Thereom to determine solutions $x(a, b)$ to each of these simultaneous equations. We know that the solution is $x = N_a H_a a + N_b H_b b$ where $N_a = m_b$, $N_b = m_a$, H_a is the multiplicative inverse of $N_a \pmod{a}$, and H_b is the multiplicative inverse of $N_b \pmod{b}$. Therefore, we know that $N_a = 11$, $N_b = 13$, $H_a = 6$, and $H_b = 6$. This means that $x(a, b) = 66a + 78b \pmod{143}$. We can list the solutions then:

$$x(1,1) = 66(1) + 78(1) = 144 \equiv 1 \pmod{143} \tag{1.3}$$
$$x(1,3) = 66(1) + 78(3) = 300 \equiv 14 \pmod{143} \tag{1.4}$$
$$x(1,5) = 66(1) + 78(5) = 456 \equiv 27 \pmod{143} \tag{1.5}$$
$$x(3,1) = 66(3) + 78(1) = 276 \equiv 133 \pmod{143} \tag{1.6}$$
$$x(3,3) = 66(3) + 78(3) = 432 \equiv 3 \pmod{143} \tag{1.7}$$
$$x(3,5) = 66(3) + 78(5) = 588 \equiv 16 \pmod{143} \tag{1.8}$$
$$x(5,1) = 66(5) + 78(1) = 408 \equiv 122 \pmod{143} \tag{1.9}$$
$$x(5,3) = 66(5) + 78(3) = 564 \equiv 135 \pmod{143} \tag{1.10}$$
$$x(5,5) = 66(5) + 78(5) = 720 \equiv 5 \pmod{143} \tag{1.11}$$

Thus we have the following solutions: $x = 1, 14, 27, 133, 3, 15, 122, 135, 5 \pmod{143}$. □

2. Problem 2

Problem 2.1. *What are the last two digits of* 2^{100} *and* 3^{100}*?*

Solution First notice that we want to find $2^{100} \pmod{100}$ in order to obtain the last two digits of 2^{100}. Also notice that the sequence $2^k \pmod{100}$ repeats itself in a cycle of length 20. We see that $2^2 \equiv 4 \pmod{100}$ and $2^{22} \equiv 4 \pmod{100}$. Therefore, it is clear that $2^{22+3*20} \equiv 2^{82} \equiv 4 \pmod{100}$. We also know that $2^{100} = 2^{82}2^{18} = 2^{82}2^{10}2^8 \equiv (4)(24)(56) \pmod{100} \equiv 76 \pmod{100}$. Therefore, the last two digits in 2^{100} are 76.

To find the last two digits in 3^{100}, we want to obtain $3^{100} \pmod{100}$. We will use a similar process. As it turns out, the sequence $3^k \pmod{100}$ repeats itself in a cycle of length 20, just as it does for the powers of 2. One can see that $3^2 \equiv 9 \pmod{100}$ and that $3^{22} \equiv 9 \mod 100$. Therefore, we see that $3^{22+3*20} \equiv 3^2 \pmod{100}$. We can also write $3^{100} = 3^{82}3^{10}3^8 \equiv (9)(49)(61) \pmod{100}$ since $3^{10} = 59049$ and $3^8 = 6561$. Thus we see that $3^{100} \equiv 1 \pmod{100}$. This the last two digits of 3^{100} are 01. □

3. Problem 3

Problem 3.1. *Find the number of solutions of $x^2 \equiv x \pmod{m}$ for any positive integer m.*

Solution First, we know that the $x^2 \equiv x \pmod{m}$ is equivalent to $x^2 - x = x(x-1) \equiv 0 \pmod{m}$. First, if m is prime, then we know there are less than or equal to 2 solutions. However, we can choose $x = 0$ and $x = 1$ which will satisfy the congruence. Thus, if m is prime, there will be two solutions.

Now, suppose m is composite. Then it can be decomposed into its prime factors: $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. If x satisfies $x(x-1) \equiv 0 \pmod{m}$ then $m|x(x-1)$ so that $p_i^{e_i}|x(x-1)$. This means that $x(x-1) \equiv 0 \pmod{p_i^{e_i}}$. Moreover, if x_i is a solution of $x(x-1) \equiv 0 \pmod{p_i^{e_i}}$ for all $i \in \{1, \dots, r\}$, then there exists a unique $x \pmod{m}$ such that:

$$x \equiv x_1 \pmod{{p_1}^{e_1}} \tag{3.1}$$

$$\vdots \tag{3.2}$$

$$x \equiv x_r \pmod{{p_r}^{e_r}} \tag{3.3}$$

This follows since we know that $p_1^{e_1}, p_2^{e_2}, \dots, p_r^{e_r}$ are relatively prime in pairs and we can therefore apply the Chinese Remainder Theorem. Now x satisfies $x(x-1) \equiv 0 \pmod{{p_i}^{e_i}}$. This shows there exists a bijection where the number of solutions to $x^2 \equiv x \pmod{m}$ is equal to the number of solutions to product of the number of solutions to $x^2 \equiv x \pmod{p_i^{e_i}}$ for all i. Thus, if we denote $N(m)$ as the number of solutions $x(x-1)$ modulo m. Thus, we see that $N(m) = N(p_1^{e_1}) \dots N(p_r^{e_r})$.

Now, to evalutate $N(p_i^{e_i})$, we must find the solutions to $x(x-1) \equiv 0 \pmod{p_i}^{e_i}$. However, we know that for any integer $x > 1$, we must have $(x, x-1) = 1$. Therefore, it must be true that if $p|x$ then $p \nmid x-1$ and conversely if $p|x-1$ then $p \nmid x$. Therefore, either $p|x$ or $p|x-1$. Moreover, we know that there are at most 2 solutions because $x^2 - x$ is of degree 2 and $p_i^{e_i}$ is a multiple of a prime. Moreover, since $x = 0, 1 \pmod{p_i}^{e_i}$ always work, we know there are exactly 2 solutions. Thus, if r is the number of unique prime factors of m, there will be 2^r solutions to $x^2 \equiv x \pmod{m}$. Since this works when m is prime and when is composite, we are done and there are 2^r solutions. □

4. Problem 4

Problem 4.1. *Show that the number $n = 561 = 3 \cdot 11 \cdot 17$ satisfies the property P: for any a coprime to n, we have $a^{n-1} \equiv 1 \pmod{n}$.*

Solution We must show that $a^{n-1} \equiv 1 \pmod{n}$ or equivalently that $a^n \equiv a \pmod{n}$. First, we know that $3, 11, 17$ are all primes so that they are pairwise coprime. This means that $a^{\phi(p)} \equiv 1 \pmod{p}$, for any $p \in \{3, 11, 17\}$ by Euler's Theorem. We know that for a prime $\phi(p) = p - 1$, so that $\phi(3) = 2$, $\phi(11) = 10$, and $\phi(17) = 16$. Moreover, we see that $(a, 3) = (a, 11) = (a, 17) = 1$ since $3, 11, 17$ are prime. Writing this out, we have:

$$a^2 \equiv 1 \pmod{3} \tag{4.1}$$

$$a^{10} \equiv 1 \pmod{11} \tag{4.2}$$

$$a^{16} \equiv 1 \pmod{17} \tag{4.3}$$

Since $a^{560} = (a^2)^{280} = (a^{10})^{56} = (a^{16})^{35}$, we see that $a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$, and $a^{560} \equiv 1 \pmod{17}$. However, since $3, 11, 17$ are coprime, the system has a unique solution with modulus $3 \cdot 11 \cdot 17 = 561$ by the Chinese Remainder Theorem. Therefore, we see that $a^{560} \equiv 1 \mod 561$, which is what we wanted. □

Problem 4.2. *Let n be a squarefree composite number satisfying P. Show that n has at least 3 prime factors.*

Solution First we will prove a small lemma which will allow us to reach a contradiction.

Lemma 4.4. *If n is a squarefree composite number satisfying P and p is a prime factor of n, then $p-1|n-1$.*

Proof. Since n is a squarefree composite number satisfying P, we know that $n|a^n - a$ for all a such that $(a, n) = 1$. This means that $p|a^n - a$ since p is a prime factor of n. However, we know that $p \nmid a$ since $(a, p) = 1$ so that $p|a(a^{n-1} - 1)$ implies $p|a^{n-1} - 1$. This shows that $a^{n-1} \equiv 1 \pmod{p}$, which means that $n - 1$ must be a multiple of $\phi(p) = p - 1$ by Fermat's Little Theorem. Thus, we see that $p - 1|n - 1$. □

Now tht we have established this lemma, we go back to our problem. If n is a squarefree composite number, then there are at least 2 prime factors. Let us assume by contradiction that there exist only 2

prime factors, let them be p and q (we cannot have $n = p^{e_p}q^{e_q}$ where $e_p, e_q > 1$ because we assumed they are squarefree. Assume without loss of generality that $p > q$. Then we use the above lemma to see that

$$p-1 \mid pq-1 \tag{4.5}$$

$$p-1 \mid p(q-1)+p-1 \tag{4.6}$$

$$p-1 \mid p(q-1) \tag{4.7}$$

Since clearly $p-1 \nmid p$, we must have $p-1|q-1$. This is a contradiciton because $p-1 > q-1$ and p, q are prime. This completes the proof □

Problem 4.3. *Write down a sufficient condition for $n = pqr$ where p, q, r are primes to satisfy property P. Then write a gp program to generate a list of ten such numbers n.*

Solution We will show that if $p = 6m+1$, $q = 12m+1$, and $r = 18m+1$ are all prime, then $n = pqr$ satisfies property P. First, we know that if p, q, r are all prime, then $a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}$ so that we have the following:

$$a^{6m} \equiv 1 \pmod{p} \tag{4.8}$$

$$a^{12tm} \equiv 1 \pmod{q} \tag{4.9}$$

$$a^{18m} \equiv 1 \pmod{r} \tag{4.10}$$

We know that p, q, r are pairwise coprime because they themselves are primes. Thus, if we can show that $6|n-1$, $12|n-1$, and $18|n-1$, then we can show that $a^{n-1} \equiv 1 \mod p, q, r$ and so that the system has a unique solution modulus $n = pqr$ by the Chinese Remainder theorem. This would show $a^{n-1} \equiv 1 \pmod{n}$ and complete the proof. Thus, we must show that $6, 12, 18|n-1 = (6m+1)(12m+1)(18m+1)-1$. Expanding out $n-1$, we have $n-1 = 1296m^3+396m^2+36m+1-1 = 1296m^3+396m^2+36m$. It is clear by inspection that $lcm(6, 12, 18) = 36$ so that $6|36$, $12|36$, and $18|36$. Since $36|396$ and $36|1296$, we see that $6m$, $12m$, and $18m$ all divide $n-1$. This completes the proof.

The following gp code returns a list of the first ten such numbers:

```
count = 0;
m = 1;
while(count<10,
    p = 6*m+1;
    q = 12*m+1;
    r = 18*m+1;
    if (isprime(p) && isprime(q) && isprime(r),
        print(p*q*r);
        count ++;
        );
    m ++;
)
```

The resulting output is:

1729
294409
56052361
118901521
172947529
216821881
228842209
1299963601
2301745249
9624742921

□

5. Problem 5

Problem 5.1. *Do there exist arbitrarily long sequences of consecutive integers, none of which are squarefree?*

Solution We will show that these arbitrarily long sequences do exist. Assume by contradiction that there exists some k such that all sequences $n, n+1, \ldots, n+k$ contain a squarefree number for all $n \in \mathbb{Z}$. Then it is clear that at least every kth integer must be squarefree. Now choose the first m primes $p_1, p_2, \ldots, p_m$

such that $p_1p_2 \dots p_m + k < p_1 \dots p_{m-1}p_{m+1}$. We shall show that for any k, we can always select an m such that this holds.

This is because for any k, we can always choose m such that $k < (p_{m+1} - p_m)(p_1 \dots p_{m-1})$ since there are infinitely many primes, and $(p_1 \dots p_{m-1})$ can be made arbitrarily large. This means that the following holds:

$$\frac{k}{p_1 \dots p_{m-1}} < p_{m+1} - p_m \tag{5.1}$$

$$p_m + \frac{k}{p_1 \dots p_{m-1}} < p_{m+1} \tag{5.2}$$

$$p_1p_2 \dots p_{m-1}p_m + k < p_1 \dots p_{m-1}p_{m+1} \tag{5.3}$$

Now let us fix m so that $p_1 \dots p_m + k < p_1 \dots p_{m-1}p_{m+1}$. First, we know that $n = p_1 \dots p_m$ must be a squarefree integer. Thus, as we have shown before, there must be another squarefree integer within the next k integers. Thus, we see that $\exists x$ for which $n < x \leq n + k$ such that x is squarefree. However, we also know that in order for x to be squarefree, it must have a prime factorization without any exponents. Moreover, we know that $x > n$. The smallest possible option for x is then $x = p_1 \dots p_{m-1}p_{m+1}$ because we must replace x_{m+1} with one of the prime factors of n (so as to not repeat a prime factor). However, we have just shown that $p_1 \dots p_m + k = n + k < p_1 \dots p_{m+1}p_{m+1} \leq x$. Thus, $n + k < x$, which is a contradiction of the fact that $n < x \leq n + k$. This completes the proof. □

6. Problem 6

Problem 6.1. *Let $f(x) = x^3 - 2$. Write a gp program to calculate the set S of primes p less than 10000 such that f has a solution modulo p. Make a conjeture about the density of such primes.*

Solution The gp code is given below. We used the first 1229 primes, since the number of primes below 10000 is 1229. This can be calculated in gp by using $primepi(10000) = 1229$.

```
numprimes = 1229;
checkprimes = primes(numprimes);
solution_count = 0;
for(i=1, numprimes,
    cprime = checkprimes[i];
    for (j=1, cprime,
        if (Mod(j^3 - 2, cprime) == Mod(0, cprime),
            solution_count ++;
            break;
        );
    );
);
print("Density: ", solution_count/numprimes);
```

We obtained 818 primes in the set S out of the 1229 possible primes. The resulting density was 0.665 for the first 1229 primes. Using the first 3000 primes, we see that the density was 0.668. Thus, I conjecture that the actual density approaches $2/3$ in the limit as $p \to \infty$. □

Problem 6.2. *Now do the same exercise for $f(x) = x^3 - 3x - 1$.*

Solution The only thing that needs to be changed in the previous code is in the if statement. Instead of using $Mod(j^2 - 2, cprime)$, we will now use $Mod(j^3 - 3j - 1, cprime)$. Running the same gp code with this change shows that there are 405 primes less than 10000 for which there exists a solution to $f(x) = x^3 - 3x - 1 \pmod p$. Thus the density is 0.329 for the first 1229 primes. Of the first 3000 primes, 1005 had solutions to $f(x) \equiv 0 \pmod p$. Thus, I conjecture that the density approaches $1/3$ in the limit as $p \to \infty$. □

Problem 6.3. *What qualitative feature of f differentiates these cases?*

Solution The polynomial $x^3 - 3x - 1$ can be factored into $x(x^2 - 3) - 1$ while $x^3 - 2$ cannot be factorized further. Thus, the first case has equivalent form of $x(x^2 - 3) \equiv 1 \pmod p$ while the second case only has the form $x^3 \equiv 2 \pmod p$. Thus, one can have $x \equiv 1 \pmod p$ or $x^2 - 3 \equiv 1 \pmod p$ in the first polynomial, but only $x^3 \equiv 2 \pmod p$ in the second polynomial. □