18.781
PROBLEM SET 4.1

JOHN WANG

1. Problem 1

Problem 1.1. *Show that the only cube root of 1 modulo 1024 is 1.*

Solution We want to solve the equation $x^3 \equiv 1 \pmod{1024}$. We will use Hansel's lemma and note that $1024 = 2^{10}$. Thus, we can find solutions to $f(x) = x^3 - 1$ in the congruence $f(x) \equiv 0 \pmod 2$ and lift solutions to $f(x) \equiv 0 \pmod{1024}$. We see that $a_1 = 1$ is the only solution to $f(x) \equiv 0 \pmod 2$ by inspection. Thus, we find that $f'(a) = 3(1)^2 \equiv 1 \pmod 2$. Thus, we see that $\overline{f'(a)} = 1 \pmod 2$. Using Hansel's lemma, we get:

$$
\begin{aligned}
a_2 &\equiv a_1 - f(a_1)\overline{f'(a)} \pmod{2^2} && (1.1)\\
&\equiv 1 - (0)(1) \pmod{2^2} && (1.2)\\
&\equiv 1 \pmod{2^2} && (1.3)\\
a_3 &\equiv 1 - (0)(1) \pmod{2^3} && (1.4)\\
&\equiv 1 \pmod{2^3} && (1.5)\\
&\vdots && (1.6)
\end{aligned}
$$

It is clear that $f(a_i) \equiv 0 \pmod{2^i}$ for all i by induction. Therefore, since $a_{i+1} \equiv a_i - f(a_i)\overline{f'(a)} \pmod{2^i} \equiv a_i \pmod{2^i}$ for all i, we know that $a_i \equiv 1 \pmod{2^i}$ for all i. By Hansel's lemma, there are no other solutions, so $x = 1 \pmod{1024}$ is the only solution to $f(x) \equiv 0 \pmod{1024}$. □

Problem 1.2. *Find all the cube roots of* -3 *modulo* 1024.

Solution We want to solve $f(x) \equiv 0 \pmod{1024} \equiv 0 \pmod{2^{10}}$ where $f(x) \equiv x^3 - 3$. First, we note that there is no solution for $f(x) \equiv 0 \pmod 2$ and small powers of 2. A solution of $a_1 = 5$ occurs for $f(x) \equiv -3 \pmod 8$. Using Hansel's lemma, we see that $a_2 \equiv 5 - (5^3 + 3)3 \pmod{16} \equiv -379 \pmod{16} \equiv 5 \pmod{16}$. If we keep going, we get:

$$
\begin{aligned}
a_3 &\equiv 5 \pmod{32} && (1.7)\\
a_4 &\equiv 5 - (5^3 + 3)3 \pmod{64} \equiv 5 \pmod{64} && (1.8)\\
a_5 &\equiv 5 - (5^3 + 3)3 \pmod{128} \equiv 5 \pmod{128} && (1.9)\\
a_6 &\equiv 5 - (5^3 + 3)3 \pmod{256} \equiv 133 \pmod{256} && (1.10)\\
a_7 &\equiv 133 - (133^3 + 3)3 \pmod{512} \equiv 133 \pmod{512} && (1.11)\\
a_8 &\equiv 133 - (133^3 + 3)3 \pmod{1024} \equiv 645 \pmod{1024} && (1.12)
\end{aligned}
$$

There are no other solutions to $f(x) \equiv 0 \pmod{1024}$, thus the only solution is $x = 645 \pmod{1024}$. □

Problem 1.3. *Solve* $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$.

Solution First, note that Hansel's lemma fails since $f(x) = x^5+x^4+1$ and $f'(x) = 5x^4+4x^3$. This means, since $a_1 = 1$ for $f(x) \pmod 3$, we have $f'(a_1) = 5+4 = 9 \equiv 0 \pmod 3$. However, we can use the construction of Hansel's lemma to attempt to proceed. We see that we must find t such that $f(a+3t) \equiv 0 \pmod{3^3}$. By the proof of Hansel's lemma, we know that a unique t occurs when $f(a) + 3tf'(a) \equiv 0 \pmod{3^2}$. Since we have already seen that $f'(a_1) = 0$, we have $f(a) \equiv 0 \pmod{3^2}$. However, since $f(a) = (1)^5+(1)^4+1 = 3 \not\equiv 0 \pmod{3^2}$, we cannot have any solutions to $f(x) \pmod{3^2}$. The same logic follows for $f(x) \pmod{3^3}$ and $f(x) \pmod{3^4}$. There there are no solutions to the congruence. □

2. Problem 2

Problem 2.1. *Write a gp program to implement Pollard rho. Use it to find a prime factor of* $2^{1231} - 1$.

Solution The Pollard rho algorithm implemented in gp uses a helper function $f(x, n)$ which just computes $f(x, n) = x^2 + 1 \pmod{n}$. The entire code is given below:

```
f(x,n)=(x^2 + 1) % n;

pr(n)=
{
    x=2;
    y=5;
    d=1;
    while(d==1,
        x=f(x,n);
        y=f(f(y,n),n);
        d=gcd(abs(y-x),n);
    );
    if (d==n, print("Failure"), print(d));
}
```

Using this algorithm on $2^{1231} - 1$, we obtain a prime factor of $p = 531,793$. □

3. Problem 3

Problem 3.1. *Suppose that* $N = pq$ *is the product of two primes. Suppose in addition to knowing* N*, we also know* $M = \phi(N)$*. Describe how you would obtain* p *and* q *from this information.*

Solution First, we know that $\phi(N) = \phi(p)\phi(q)$ because p and q are prime factors of N. Moreover, since p, q are primes, we know that $\phi(p) = p-1$ and $\phi(q) = q-1$. Thus, we see that $M = \phi(N) = (p-1)(q-1) = pq - p - q + 1 = N - p - q + 1$. From this, we see that $p = N - M - q + 1$. Since $pq = N$, we see that the following is true:

$$N = pq = (N - M - q + 1)q \tag{3.1}$$
$$0 = q^2 + q(M - N) + N - 1 \tag{3.2}$$

This is a quadratic in q, which can be solved using the quadratic formula:

$$q = \frac{-(M-N) \pm \sqrt{(M-N)^2 - 4(N-1)}}{2} \tag{3.3}$$

Then, we can use q to figure out p by using $p = N/q$. However, notice that p will simply be the other solution of the quadratic since p and q are symmetric so their quadratic equations will be the same.
□

Problem 3.2. *Use the above method to factor the number:*

$$N = 2760698538716225514973902344910793166845871614262060116995480300080332 9 \tag{3.4}$$

which is a product of two primes given that:

$$\phi(N) = 27606985387162255149739023449107761527112996396559656119259509106409476 \tag{3.5}$$

Solution We will run the above algorithm. Solving the equation, we obtain:

$$q = 16225927682921336339157801028812 7 \tag{3.6}$$
$$p = 1701411834604692317316873037158841057 27 \tag{3.7}$$

A check check using gp shows that both p and q are prime numbers, and that $pq = N$. □

4. Problem 4

Problem 4.1. *Suppose that $f(x) \equiv 0 \pmod{p^j}$ and that $f'(a) \not\equiv 0 \pmod p$. Let $\overline{f'(a)}$ be an integer chosen so that $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^{2j}}$ and set $b = a - f(a)\overline{f'(a)}$. Show that $f(b) \equiv 0 \pmod{p^{2j}}$.*

Solution First, we will use a small lemma, which is very close to the lemma proven in class:

Lemma 4.1. *If $j \geq 1$ then $f(a + tp^j) = f(a) + tp^j f'(a) \pmod{p^{2j}}$.*

Proof. We will use a Taylor expansion about a to find that:

$$f(a+tp^j) = f(a) + tp^j f'(a) + (tp^j)^2 \frac{f''(a)}{2!} + \dots \tag{4.2}$$

$$= f(a) + tp^j f'(a) \pmod{2^{2j}} \tag{4.3}$$

The second line follows because $f''(a)/2! = (k)(k-1)a^{k-2}/2 = \binom{k}{2}a^{k-2} \in \mathbb{Z}$. Moreover, each term $f^{(r)}(a)/r!$ is an integer because $f^{(r)}(a)/r! = \binom{k}{r}a^{k-r}$ using the logic from above. Therefore, we see that all these terms are integers, and that $p^{2j}, p^{3j}, p^{4j}, \dots$ are all divisible by p^{2j}. Therefore, the terms:

$$(tp^j)^2 \frac{f''(a)}{2!} + (tp^j)^3 \frac{f'''(a)}{3!} + \dots \equiv 0 \pmod{2^j} \tag{4.4}$$

This completes the proof of the lemma. $\square$

Now that we have this result, we want to find a t such that $0 \equiv f(a) + tp^j f'(a) \pmod{p^{2j}}$. Rearranging terms, we can solve for t and we find that $t \equiv -\frac{f(a)}{p^j}\overline{f'(a)} \pmod{2j}$. We know that this is an integer because $f(a) \equiv 0 \pmod{p^j}$ so that $p^j | f(a)$ and so $\frac{f(a)}{p^j}$ is an integer. Moreover, we see the following with this result:

$$a + tp^j = a + \frac{f(a)}{p^j}\overline{f'(a)}p^j = a + f(a)\overline{f'(a)} = b \tag{4.5}$$

Thus, we have shown that b satisfies $f(b) \equiv 0 \pmod{p^{2j}}$. $\square$

5. problem 5

Problem 5.1. *Let p be a prime. Let $\sigma_1, \sigma_2, \dots, \sigma_{p-1}$ be the elementary symmetric polynomials in $1, 2, \dots, p-1$ as in class (i.e. σ_k is the sum of products of k of these numbers). We showed that $(-1)^{p-1}\sigma_{p-1} = (p-1)! \equiv -1 \pmod p$. Show that $\sigma_1, \dots, \sigma_{p-2}$ are all congruent to $0 \pmod p$.*

Solution We showed in class that the following congruence must hold:

$$(x-1)(x-2)\dots(x-(p-1)) \equiv x^{p-1} - 1 \pmod p \tag{5.1}$$

However, we also showed in class that if we have a product $f(x) = (x - \alpha_1)\dots(x - \alpha_p)$ where $\alpha_i \in \{1, 2, \dots, p-1\}$, then we have $f(x) = x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} + \dots + (-1)^{p-1}\sigma_{p-1}$. Thus, the following congruence must hold:

$$x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} + \dots + (-1)^{p-1}\sigma_{p-1} \equiv x^{p-1} - 1 \pmod p \tag{5.2}$$

Since we know that the constant term on the left hand side is $(-1)^{p-1}\sigma_{p-1} \equiv -1 \pmod p$, we can subtract $x^{p-1} - 1$ from both sides. Using this observation, we obtain:

$$-\sigma_1 x^{p-2} + \sigma_2 x^{p-3} + \dots + (-1)^{p-2}\sigma_{p-2}x \equiv 0 \pmod p \tag{5.3}$$

However, each one of these terms is a different power of x. Since this congruence must hold for all x, we know that the coefficients on each of the x^i terms must be equivalent to $0 \pmod p$. This shows that $\sigma_1, \dots, \sigma_{p-2}$ are all congruent to $0 \pmod p$. $\square$

Problem 5.2. *For $p \geq 5$, show that $\sigma_{p-2} \equiv 0 \pmod{p^2}$.*

Solution As we noted before, we know that the following equation holds from lecture:

$$(x-1)(x-2)\dots(x-(p-1)) = x^{p-1} - \sigma_1 x^{p-2} + \dots + \sigma_{p-1} \tag{5.4}$$

Now, we let $x = p$, and we find the following:

$$(p-1)(p-2)\dots(p-(p-1)) = p^{p-1} - \sigma_1 p^{p-2} + \dots + \sigma_{p-1} \tag{5.5}$$

$$(p-1)! = p^{p-1} - \sigma_1 p^{p-2} + \dots + \sigma_{p-1} \tag{5.6}$$

Since we know that $(-1)^{p-1}\sigma_{p-1} = (p-1)!$ from lecture and from the statement of the problem, we see that we can rearrange the above expression and cancel out σ_{p-1} (since $(-1)^{p-1} = 1$ as $p-1$ is even). This gives:

$$0 = -\sigma_1 p^{p-2} + \sigma_2 p^{p-3} + \ldots - \sigma_{p-3}p^2 + \sigma_{p-2}p \tag{5.7}$$

(5.8)

Since $\sigma_i \in Z$, if we take everything modulo p^2, we notice that $p^2|p^i$ for all $i \geq 2$. These two facts imply that $(-1)^i\sigma_{i+1}p^i \equiv 0 \pmod{p^2}$ for all $i > 2$. This implies that:

$$\sigma_{p-2} \equiv 0 \pmod{p^2} \tag{5.9}$$

This completes the proof. □

6. Problem 6

Problem 6.1. *Let p be a prime, and g a primitive root modulo p. Show that $1, g, g^2, \ldots, g^{p-2}$ are all the nonzero residue classes mod p.*

Solution First, since g is a primitive root modulo p, we know that $ord_p(g) = p-1$. Therefore, we see that $p-1$ is the lowest power $k > 0$ such that $g^k \equiv 1 \pmod{p}$. If we can show that $1, g, g^2, \ldots, g^{p-2}$ are all distinct modulo p, then we know that they constitute all the non-zero residue classes modulo p. Suppose not. Then there exist integers i and j such that $0 \leq i \neq j \leq p-2$ such that $g^i \equiv g^j \pmod{p}$. Without loss of generality, assume that $i > j$. We see that this implies $g^{i-j} \equiv 1 \pmod{p}$ using division by the greatest common divisor. However, we know that $i - j < p - 1$. However, we know that $ord_p(g) = p-1$, which is a contradiction because $i - j$ is a smaller power which satisfies $g^k \equiv 1 \pmod{p}$. □

Problem 6.2. *For a positive integer k, let $S_k = 1^k + 2^k + \ldots + (p-1)^k$. Compute the value of S_k modulo p in closed form as a function of k.*

Solution First, we note that if $k \equiv p-1 \pmod{p}$, then we must have $i^k \equiv i^{\phi(p)} \equiv 1 \pmod{p}$ for all $i \in \{1, 2, \ldots, p-1\}$ using Euler's Theorem. Since there are $p-1$ of these terms in the sum, we find that $S_{p-1} \equiv p-1 \pmod{p}$.

Now suppose that k is not a multiple of $p-1$. Then let g be a primitive root of modulo p, which we know exists because p is prime. Using the result that we have proven above, we know that $1, g, g^2, \ldots, g^{p-2}$ are all the nonzero residue classes modulo p. Thus, we know that the above set is just a reordering of $1, 2, 3, \ldots, p-1$. This means we can write:

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} (g^i)^k \pmod{p} \tag{6.1}$$

$$\equiv \sum_{i=1}^{p-1} (g^k)^i \pmod{p} \tag{6.2}$$

$$\equiv \frac{g^k((g^k)^{p-1} - 1)}{g^k - 1} \pmod{p} \tag{6.3}$$

Where the last line comes from the expression for a finite geometric series. However, since we know that $(g^k)^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem, we know that the entire sum comes out to zero. Moreover, we know that the denominator is not zero because $p - 1 \nmid k$ by assumption, so that $g^k \not\equiv 1 \pmod{p}$. This shows that $S_k = 0$ for all k such that $p - 1 \nmid k$. We then have the following formula:

$$S_k \equiv \begin{cases} p-1 \pmod{p} & \text{if } k \equiv 0 \pmod{p} \\ 0 \pmod{p} & \text{otherwise} \end{cases} \tag{6.4}$$

□