Math 437 Homework 3

Xander Naumenko

07/11/23

Question 1. We are trying to find instances of when $a_n \equiv 0 \mod 2023$, so consider the recurrence relation $\mod 2023$. All future values of the sequence are determined by the 5-tuple $(a_n, a_{n+1}, a_{n+2}, n^2, 5^n)$, each value within being modulo 2023. There are 2023 possibilities for the first 4 and $\text{ord}_{2023}5 = 816$ possibilities for the last, so by the pigeonhole principle the sequence must repeat after at most $2023^4 \cdot 816 \approx 1.367 \cdot 10^{16}$ steps. Since it repeats infinitely from then on out, all we must do is show that there is at least one 0 within the repeating section. I claim that $a_0 = 0$ is in the repeating section which fulfills this requirement.

To see why, let p be the period of repetition (i.e. the smallest number such that $a_m \equiv a_{m+p}, 5^m \equiv 5^{m+p}, m^2 \equiv (m+p)^2 \mod 2023$ for all m sufficiently large, this is guaranteed to exist as shown above) and n be the smallest number such that $a_m \equiv a_{m+p}, 5^m \equiv 5^{m+p}, m^2 = (m+p)^2 \mod 2023 \forall m \geq n$. In particular, $a_n \equiv a_{n+p}, a_{n+1} \equiv a_{n+p+1}, a_{n+2} \equiv a_{n+p+2} \mod 2023$. Note that $816|p$ and $2023|p$ due to the 5^m and m^2 requirement and the fact that 2023 isn't a perfect square. Then consider a_{n-1}, using the fact that $11 \cdot 184 \equiv 1 \mod 2023$:

$$a_{n-1} \equiv 184\left(a_{n+2} - 5^n a_{n+1} - n^2 a_n\right) \equiv 184\left(a_{n+p+2} - 5^{n+p} a_{n+p+1} - (n+p)^2 a_{n+p}\right) \mod 2023$$

$$\equiv a_{n+p-1} \mod 2023.$$

Since $5^{n-1} \equiv 1214 \cdot 5^n \equiv 1214 \cdot 5^{n+p} \equiv 5^{n+p-1} \mod 2023$ and $(n-1)^2 \equiv n^2 - 2n + 1 \equiv (n+p)^2 - 2(n+p) + 1 \equiv (n+p-1)^2 \mod 2023$, this contradicts our assumption that n was chosen to be minimal. The only way this doesn't lead to a contradiction is if $n = 0$ as $a_{n-1} = a_{-1}$ isn't defined. Thus $a_0 \equiv 0 \mod 2023$ is in the repetition and $2023|a_n$ infinitely many times. $\square$

While this concludes the proof, alternatively to carefully proving that a_0 is in the repeating section one also could have just brute force searched for a repeating 5-tuple in the form above and checked that the repeating section contains a zero. Here's some python code to do so, it turns out to repeat with period $p = 4660992$ and $n = 0$ as expected.

```
N = 10000000
a = [0,1,2] + [0]*(N-3)

seen = {}
repeat_n = -1
repeat_h = ()

for n in range(0,N-3):
    a[n+3] = (5**(n%816)*a[n+2]+n**2*a[n+1]+11*a[n])%2023
    h = (n%816,(n**2)%2023,a[n+2],a[n+1],a[n])
    if h in seen:
        print(f'Found at n={n}')
```

```
        repeat_n = n
        repeat_h = h
        break
    seen[h] = n

if repeat_n == -1:
    print('No repeat found')
else:
    n1 = seen[repeat_h]
    n2 = repeat_n
    print(f'Found repeat at n1={n1}, n2={n2}')
    print(repeat_h)
    print('Searching for zeros...')
    for n in range(n1,n2+1):
        if a[n] == 0:
            print(f'Found zero at n={n}')
            print(f'Sanity check: n1={n1}, a[{n1}]={a[n1]}, a[{n1}+1]={a[n1+1]}, a
                ↪ [{n1}+2]={a[n1+2]}, (5^({n1}))%2023={(5**n1)%2023}, ({n1}^2)
                ↪ %2023={(5**n1)%2023}')
            print(f'Sanity check: n2={n2}, a[{n2}]={a[n2]}, a[{n2}+1]={a[n2+1]}, a
                ↪ [{n2}+2]={a[n2+2]}, (5^({n2}))%2023={(5**n2)%2023}, ({n2}^2)
                ↪ %2023={(5**n2)%2023}')
            break
```

Question 2. Factor n as $n = 2^{\alpha_0}\prod_{i=1}^{r} p_i^{\alpha_i}$ with the p_i being odd primes. Let $P(x) = x^3 - 1$, as proven in theorem 8.2, it is sufficient to find $N_P(p_i^{\alpha_i})$ and $N_P(2^{\alpha_0})$, then multiply them all together to find $N_P(n)$. Proposition 18.2 from the notes tells us that the number of solutions to $x^m \equiv a \mod p^\alpha$ is

$$\begin{cases} 0 & \text{if } a^{\frac{\phi(p^\alpha)}{\gcd(m,\phi(p^\alpha))}} \not\equiv 1 \mod p^\alpha \\ \gcd(m,\phi(p^\alpha)) & \text{if } a^{\frac{\phi(p^\alpha)}{\gcd(m,\phi(p^\alpha))}} \equiv 1 \mod p^\alpha \end{cases}.$$

Since in this case $a = 1, m = 3$, this reduces to $N_P(p_i^{\alpha_i}) = \gcd(3, \phi(p_i^{\alpha_i})) = 3$ if $3|p_i^{\alpha_i - 1}(p_i - 1), 1$ otherwise. For the 2^{α_0} factor we can't apply Proposition 18.2 since it only applies to odd primes, so another argument is needed. Consider $\phi(2^n)$, since half the numbers less than 2^n are even and the other half are odd, $\phi(2^n) = 2^{n-1}$. However $3 \nmid 2^{n-1} \forall n$, so the only solution to $x^3 \equiv 1 \mod 2^{\alpha_0}$ is $x \equiv 1 \mod 2^{\alpha_0}$. Multiplying these all together, we get that

$$N_P(n) = N_P(2^{\alpha_0})\prod_{i=1}^{r} N_P(p_i^{\alpha_i}) = 3^{\#\text{ of } i \text{ s.t. } 3|p_i^{\alpha_i - 1}(p_i - 1)}. \square$$

To double check that this correctly counts everything once again one can write a quick python script:

```
from sympy import factorint

n = 2**3 * 3**3 * 5**2 * 7**2 * 79

def brute_force_count(n):
```

```
    count = 0
    for i in range(n):
        if i**3 % n == 1:
            count += 1
    return count

def smart_count(n):
    factors = factorint(n)
    count = 1
    for p,alpha in factors.items():
        if p == 2:
            continue
        if p**(alpha-1)*(p-1)%3 == 0:
            count *= 3
    return count

print(brute_force_count(n), smart_count(n))
```

Question 3. I will construct the sequence $\{n_k\}_{k\geq 1}$ and show that the sequence is valid. They will be in the form $n_k = \prod_{i=1}^{k} p_i^{a_i}$, p_i is the ith prime and $a_i \in \{0,1\}$ are shared between all n_k (i.e. a_i isn't a function of k), so the sequence a_i uniquely defines the sequence n_k.

Let $\alpha \in [0,1]$. Note that for n_k in the form above we have $n_k = p_k^{a_k} n_{k-1}$. Let $a_k = 1$ if $\left(1-\frac{1}{p_k}\right)\prod_{i=1}^{k-1}\left(1-\frac{1}{p_i}\right)^{a_i} \geq \alpha$ and $a_k = 0$ otherwise. I claim that these a_k define a sequence n_k that fulfills the required limit.

If $\alpha = 1$ then $n_k = 1$ works, so assume $\alpha < 1$. Let $\epsilon > 0$, and to make some of the algebra later simpler assume that $\epsilon < 1 - \alpha$. Expanding out the given limit using the fact that $a_i \in \{0,1\}$, we have

$$\lim_{k\to\infty} \frac{\phi(n_k)}{n_k} = \prod_{i=1}^{\infty}\left(\frac{p_i - 1}{p_i}\right)^{a_i} = \prod_{i=1}^{\infty}\left(1-\frac{1}{p_i}\right)^{a_i}.$$

The product is decreasing and the a_is were specifically constructed so that each of these partial products are always greater than α, so all that needs to be shown is that there is some partial product that is smaller than $\alpha+\epsilon$. Before this can be done, first note that $\prod_{i=1}^{\infty}\left(1-\frac{1}{p_i}\right) = 0$ (this relies on some slightly non-rigorous expansion but something very similar was shown in class so I assume it's fine):

$$\prod_{i=1}^{\infty}\left(1-\frac{1}{p_i}\right) = \left(\prod_{i=1}^{\infty}\frac{1}{1-p_i^{-1}}\right)^{-1} = \left(\prod_{i=1}^{\infty} 1 + p_i^{-1} + p_i^{-2} + \dots\right)^{-1} = \left(\sum_{i=1}^{\infty}\frac{1}{i}\right)^{-1} = \frac{1}{\infty} = 0.$$

Let K be such that $\frac{1}{p_K} < \epsilon$ and denote $A = \prod_{i=1}^{K}\left(1-\frac{1}{p_i}\right)^{a_i}$. If $A < \alpha + \epsilon$ already then we're done, so assume it isn't. Then since $\prod_{i=1}^{\infty}\left(1-\frac{1}{p_i}\right) = 0$ there exists an N such that $B = A\prod_{i=K+1}^{N}\left(1-\frac{1}{p_i}\right) < \alpha+\epsilon$, also assume that N is chosen to be the smallest possible that fulfills this property. By the minimality of N we have that $B\left(1-\frac{1}{p_N}\right)^{-1} \geq \alpha+\epsilon$, so using the fact that $\alpha+\epsilon \leq 1$ we get

$$B \geq (\alpha+\epsilon)\left(1-\frac{1}{p_N}\right) \geq (\alpha+\epsilon)\left(1-\frac{1}{p_K}\right) \geq (\alpha+\epsilon)(1-\epsilon) \geq \alpha+\epsilon-\epsilon = \alpha.$$

Thus $B \in [\alpha, \alpha + \epsilon)$. Then by the construction of a_i we have that $a_{K+1} = \ldots = a_N = 1$, so $B = A \prod_{i=K+1}^{N} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{a_i} = \frac{\phi(n_N)}{n_N} \in [\alpha, \alpha + \epsilon)$. Since $\frac{\phi(n_k)}{n_k}$ is bounded below by α, is decreasing and comes arbitrarily close to α, its limit is α. $\square$