PUMaC 2015

Number Theory A

1. [**3**] What is the 22nd positive integer n such that 22^n ends in a 2? (when written in base 10).

   Solution:

   The last digits of the powers of 22 cycle $2, 4, 8, 6, 2, 4, 8, 6, \ldots$. The answer is thus the 22nd term of the arithmetic sequence $1, 5, 9, \ldots$, which is $\boxed{85}$.

   Author: Eric Neyman

2. [**3**] What is the sum of all positive integers n such that $\text{lcm}(2n, n^2) = 14n - 24$?

   Solution:

   $\text{lcm}(2n, n^2)$ is n^2 when n is even and $2n^2$ when n is odd. Solving the equation $n^2 = 14n - 24$, we get $n = 2$ and $n = 12$, both of which are even and thus yield solutions. Solving $2n^2 = 14n - 24$, we get $n = 3$ and $n = 4$, of which only $n = 3$ works, because it is odd. Thus, our answer is $2 + 3 + 12 = \boxed{17}$.

   Author: Eric Neyman

3. [**4**] What is the largest positive integer n less than $10,000$ such that in base 4, n and $3n$ have the same number of digits; in base 8, n and $7n$ have the same number of digits; and in base 16, n and $15n$ have the same number of digits? Express your answer in base 10.

   Solution:

   The conditions are basically stating that in each of the three bases, n must appear "alphabetically" before $1111\ldots$. Let k_4, k_8, and k_{16} be the largest positive integers such that $4^{k_4} < n$, $8^{k_8} < n$, and $16^{k_{16}} < n$. Then $n < 2 \cdot 4^{k_4}$, $n < 2 \cdot 8^{k_8}$, and $n < 2 \cdot 16^{k_{16}}$. In other words, $n < 2^{2k_4+1}$, $n < 2^{3k_8+1}$, and $n < 2^{4k_{16}+1}$, but $n > 2^{2k_4}$, $n > 2^{3k_8}$. and $n > 2^{4k_{16}}$. It follows that the greatest power of 2 that is less than n must be 2^{12k} for some integer k (because 12 is the least common multiple of 2, 3, and 4). The largest such k can be 1 if n is to be less than $10,000$. From here it is easy to see that the largest possible value of n is the smallest of 1111_{16}, 11111_8, and 1111111_4, and that is $1111_{16} = \boxed{4369}$.

   Author: Eric Neyman

4. [**4**] What is the smallest positive integer n such that $20 \equiv n^{15} \pmod{29}$?

   Solution:

   By Fermat's Little Theorem, $a^{28} \equiv 1 \pmod{29}$ for all positive integers a that are not multiples of 29. It follows that $a^{14} \equiv \pm 1 \pmod{29}$, so $a^{15} \equiv \pm a \pmod{29}$ for all such a. Thus, if $a^{15} \equiv 20 \pmod{29}$, then $\pm a \equiv 20 \pmod{29}$. We know that $9^{14} = 3^{28} \equiv 1 \pmod{29}$, so $9^{15} \equiv 9 \pmod{29}$. Next we try $a = 20$, and we find that $20^{14} \equiv 49^{14} \equiv 7^{28} \equiv 1 \pmod{29}$, and so $20^{15} \equiv 20 \pmod{29}$. Therefore, the smallest such a is $\boxed{20}$.

   Author: Heesu Hwang

5. [**5**] Given that there are 24 primes between 3 and 100, inclusive, what is the number of ordered pairs (p, a) with p prime, $3 \le p < 100$, and $1 \le a < p$ such that the sum

$$a + a^2 + a^3 + \cdots + a^{(p-2)!}$$

is not divisible by p?

Solution:

If $a = 1$, then the sum just becomes $(p-2)!$, which is never divisible by p. So since there are 24 odd primes between 2 and 100, there are 24 solutions of the form $(p, 1)$.

Next, suppose $a \neq 1$. The sum can then be written as

$$a + a^2 + \cdots + a^{(p-2)!} = a\frac{a^{(p-2)!} - 1}{a-1} = \frac{a}{a-1} \cdot (a^{(p-2)!} - 1).$$

Since $1 < a < p$, the term $a/(a-1)$ does not contribute to whether the sum is divisible by p. So it suffices to consider the term $a^{(p-2)!} - 1$. Now look at the following cases.

(a) If $p = 3$, then the sum is just a which isn't divisible by p. So $(3, 2)$ is a valid solution.

(b) If $p = 5$, then the sum is just

$$\frac{a}{a-1} \cdot (a^6 - 1) \equiv \frac{a}{a-1} \cdot (a^2 - 1) \equiv a(a+1) \pmod p$$

by Fermat's Little Theorem. Plugging in $a = 2, 3, 4$ shows that $(5, 2)$ and $(5, 3)$ are the only solutions here.

(c) If $p > 5$, then $2 \neq (p-1)/2$. Moreover, we also have $2 \mid (p-2)!$ and $(p-1)/2 \mid (p-2)!/2$ since $1 < 2, (p-1)/2 < p-2$. Thus $(p-1) \mid (p-2)!$, so by Fermat's Little Theorem $a^{(p-2)!} - 1 \equiv 0 \pmod p$. Thus the sum is always divisible by p in this case, and there are no solutions here.

Thus there is a total of $\boxed{27}$ solutions.

Author: Steven Kwon

6. [**6**] For a positive integer n, let $d(n)$ be the number of positive divisors of n. What is the smallest positive integer n such that

$$\sum_{t|n} d(t)^3$$

is divisible by 35?

Solution:

First, one can check that if $n = \prod_{i=1}^{k} p_i^{e_i}$ is its prime factorization (with each p_i distinct and $1 \le e_i \le k$), then $d(n) = \prod_{i=1}^{k}(e_i+1)$. So, we see that $\gcd(a, b) = 1 \implies d(ab)^3 = d(a)^3 d(b)^3$. This implies that if $t = \prod_{i=1}^{k} p_i^{f_i}$ where $0 \le f_i \le e_i$,

$$\sum_{t|n} d(t)^3 = \sum_{t|n} \prod_{i=1}^{k} d(p_i^{f_i})^3 = \prod_{i=1}^{k} \sum_{s|p_i^{f_i}} d(s)^3 = \prod_{i=1}^{k} \sum_{j=0}^{e_i} (j+1)^3.$$

Above, we used the fact that as t ranges over the divisors of n, the exponents f_i each range from 0 to e_i. Therefore, using the well-known identity that $\sum_{i=0}^{n} i^3 = (\sum_{i=0}^{n} i)^2$, the above becomes

$$\prod_{i=1}^{k} \left(\sum_{j=0}^{e_i} (j+1) \right)^2 = \prod_{i=1}^{k} \left(\frac{(c_i+1)(c_i+2)}{2} \right)^2.$$

For this expression to be divisible by 35, we need $(c_i+1)(c_i+2)$ to be divisible by 5 for some i and by 7 for some i. If these are two different values of i, the smallest possible values are 3 and 5, respectively. Setting $c_1 = 3$, $c_2 = 5$, $p_1 = 3$, and $p_2 = 2$ gives the smallest possible value of n in this case, which is $2^5 \cdot 3^3 = 864$. If the two values of i are the same, then the smallest possible value of c_i such that $(c_i+1)(c_i+2)$ is divisible by both 5 and 7 is if $c_i = 13$. Setting $p = 2$, this yields $n = 2^{13} > 864$. Thus, the answer is $\boxed{864}$.

Authors: Steven Kwon, Eric Neyman

7. [**7**] Given a positive integer k, let $f(k)$ be the sum of the k-th powers of the primitive roots of 73. For how many positive integers $k < 2015$ is $f(k)$ divisible by 73?

Note: A primitive root r of a prime p is an integer $1 \le r < p$ such that the smallest positive integer k such that $r^k \equiv 1 \pmod p$ is $k = p-1$.

Solution:

Denote S_d^k to be the sum of the k-th powers of the residues of order d modulo $p = 73$. Now, for any primitive root r of p, we have:

$$\mathrm{ord}_p(r^k) = \frac{\mathrm{ord}_p(r)}{\gcd(k, p-1)} = \frac{p-1}{\gcd(k,p-1)} = d_k$$

Furthermore, the number of residues of p of order d is:

$$n_d = \phi(d)$$

Now, since d_k is independent of the primitive root r, S_1^k is equal to a sum of n_{p-1} residues of order d_k. More specifically, due to symmetry within the group $\mathbb{Z}/p\mathbb{Z}$, each residue or order d_k is represented in the sum the same number of times. Then, we have:

$$S_1^k = \frac{n_{p-1}}{n_{d_k}} \cdot S_{d_k} = \frac{\phi(p-1)}{\phi\big(\frac{p-1}{\gcd(k,p-1)}\big)} \cdot S_{d_k} = \phi\big(\gcd(k,p-1)\big) \cdot S_{d_k}$$

Clearly, $p \nmid \phi\big(\gcd(k,p-1)\big) < p$, so $p \mid S_{d_k}$. We now present a lemma:

<u>Lemma 1:</u> For some $d \mid p-1$, $S_d \equiv 0 \pmod p$ iff d is divisible by a perfect square. Furthermore, if $d = q_1 q_2 \dots q_m$ is square-free, then we have that $S_d \equiv (-1)^m$.

Proof: We prove by induction. For $d = 1$, it is clear that $S_1 = 1 = (-1)^0$. Now, assume this is true for all $d' < d$. Let x be a residue of order d modulo p. Clearly, $p \mid x^{d-1} + x^{d-2} + \ldots + x + 1$, as $p \mid x^d - 1$ by assumption and $p \nmid x - 1$. But, we have:

$$x^{d-1} + x^{d-2} + \ldots + x + 1 = \sum_{d' \mid d} S_{d'} \equiv 0 \pmod p$$

If d is square-free, we write $d = q_1 q_2 \dots q_m$. Then, we have:

$$S_d \equiv -\sum_{d' \mid d, d' \neq d} S_{d'} \equiv (-1)\left(\sum_{i=0}^{m-1} (-1)^i \binom{m}{i}\right) \equiv (-1)\left(-(-1)^m \binom{m}{m}\right) \equiv (-1)^m \pmod p$$

Otherwise, we write $d = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_m^{\alpha_m}$ and $e = q_1 q_2 \dots q_m < d$. Then, we have:

$$S_d \equiv -\sum_{d'|d, d' \neq d} S_{d'} \equiv -\sum_{e'|e} S_{e'} \equiv (-1)\left(\sum_{i=0}^{m} (-1)^i \binom{m}{i}\right) \equiv 0 \pmod p$$

As desired. □

This means that k satisfies the condition iff d_k is divisible by a perfect square. Since $p - 1 = 72 = 2^3 \cdot 3^2$, d_k is square-free iff $2^2 \cdot 3 = 12 \mid k$, so k satisfies the condition iff $12 \nmid k$. There are $2014 - \lfloor \frac{2014}{12} \rfloor = \boxed{1847}$ such k.

Author: Bill Huang

8. [**8**] Let $n = 2^{2015} - 1$. For any integer $1 \leq x < n$, let

$$f_n(x) = \sum_p s_p(n - x) + s_p(x) - s_p(n),$$

where $s_q(k)$ denotes the sum of the digits of k when written in base q and the summation is over all primes p. Let N be the number of values of x such that $4 \mid f_n(x)$. What is the remainder when N is divided by 1000?

Solution:

First, observe that for any integer k and prime p, the number of times p divides $k!$ is:

$$v_p(k!) = \frac{k - s_p(k)}{p - 1}$$

Then, we find that:

$$\begin{aligned} v_p\left(\binom{n}{x}\right) &= v_p\left(\frac{n!}{x!(n-x)!}\right) \\ &= \frac{\big(n - s_p(n)\big) - \big(x - s_p(x)\big) - \big((n - x) - s_p(n - x)\big)}{p - 1} \\ (p-1)v_p\left(\binom{n}{x}\right) &= s_p(n - x) + s_p(x) - s_p(n) \end{aligned}$$

Now, since $n = 2^{2015} - 1$, it is clear that $2 \nmid \binom{n}{x}$ for any x, so in any non-zero term in the summation, $p - 1$ is always even. Let $\mathcal{P}_i$ be the set of primes $p \equiv i(\bmod 4)$. We then have that $4|p - 1$ when $p \in \mathcal{P}_1$, so we only need to worry about the primes $p \in \mathcal{P}_3$.

Now, taking the summation of each $p \in \mathcal{P}_3$ term modulo 4, the problem is reduced to proving that:

$$2 \,\Bigg|\, \sum_{p \in \mathcal{P}_3} v_p\left(\binom{n}{x}\right)$$

Now, note that the product of an even number of primes $p \in \mathcal{P}_3$ is equivalent to $1(\bmod 4)$ and an odd number $3(\bmod 4)$. Thus, the above statement is equivalent to:

$$\binom{n}{x} \equiv 1(\bmod 4)$$

For $x < \frac{n}{2}$, we have:

$$\prod_{i=1}^{x} \frac{n-i+1}{i} \equiv (-1)^x (\text{mod} 4)$$
$$1 \equiv (-1)^x (\text{mod} 4)$$

Which means that x is even, so there are $\left\lfloor \frac{\lfloor \frac{n}{2} \rfloor}{2} \right\rfloor = 2^{2013} - 1$ values of $x < \frac{n}{2}$ that satisfy the condition. Since $\binom{n}{x}$ is symmetric about $\frac{n}{2}$, the total number of x that satisfy the condition is $2^{2014} - 2$.

Note that $2^n \equiv 0 \pmod 8$ for $n \geq 3$ and that, by the Euler-Fermat Theorem, $2^{\phi(125)} = 2^{100} \equiv 1 \pmod{125}$. From this we conclude that $2^{2014} - 2 \equiv 2^{14} - 2 \equiv 16384 - 2 \equiv \boxed{382} \pmod{1000}$.

Author: Bill Huang