MATH 152 Problem set 2 solutions

p or p_i denotes a prime number.

1. Let l be the order of 10 in $\mathbb{Z}/p\mathbb{Z}$. (Such l exists because $(10, p) = 1$ by assumption.) Then $10^l \equiv 1 \pmod p$, and

$$\begin{aligned} 10^l &= 1 + cp \text{ for some } c < 10^l \\ \Rightarrow \quad p &= \frac{10^l - 1}{c} \\ \Rightarrow \quad \frac{1}{p} &= c \cdot \frac{1}{10^l - 1} = \frac{c}{10^l} \cdot \frac{1}{1 - 10^l} \\ \Rightarrow \quad \frac{1}{p} &= \frac{c}{10^l}\Big(1 + \frac{1}{10^l} + \frac{1}{10^{2l}} + \dots\Big) \\ \Rightarrow \quad \frac{1}{p} &= \frac{c}{10^l} + \frac{c}{10^{2l}} + \frac{c}{10^{3l}} \dots \end{aligned}$$

Since $c < 10^l$, c has no more than l digits. Write c in the decimal expansion $c = \sum_{i=0}^{l-1} c_i 10^i$, where $0 \le c_i \le 9$. Substituting this to the last equality above, we have

$$\frac{1}{p} = \frac{c_l}{10^1} + \frac{c_{l-1}}{10^2} + \dots + \frac{c_0}{10^l} + \frac{c_l}{10^{l+1}} + \dots + \frac{c_0}{10^{2l}} + \frac{c_l}{10^{2l+1}} + \dots + \frac{c_0}{10^{3l}} + \dots$$

2. (a) $d_N = \prod_{p_i \text{ prime}} p_i^{\alpha_i}$, where $\alpha_i = \max\{\alpha : p_i^\alpha \mid n, 1 \le n \le N\} = \max\{\alpha : p_i^\alpha \le N\} = \lfloor \frac{\log N}{\log p} \rfloor$. Therefore, taking logarithms, we obtain

$$\log d_N = \sum_{p \le N} \log p \Big\lfloor \frac{\log N}{\log p} \Big\rfloor.$$

Since $\lfloor \frac{\log N}{\log p} \rfloor \le \frac{\log N}{\log p}$, the right-hand side is less than or equal to

$$\sum_{p \le N} \log p \frac{\log N}{\log p} = \sum_{p \le N} \log N = (\log N)\pi(N),$$

as desired.

(b) First let's compute the integral:

$$d_N \int_0^1 f(x)dx = \Big[d_N a_0 x + d_N \frac{a_1}{2} x^2 + \dots + d_N \frac{a_{N-1}}{N} x^N\Big]_0^1.$$

Note that $n \mid d_N$ for all $1 \leq n \leq N$. Therefore the right-hand side is an integer.

(c) Because of (b), all we need to show is that the integral is strictly positive, that is, strictly greater than zero. This is easily seen to be true because $f(x) > 0$ for all $x \in (0,1)$.

(d) f_N is nonnegative and bounded by 4^{-N} on $[0,1]$. Therefore $\int_0^1 f_N(x)dx \leq 4^{-N}$.

Next, by (c) we have $4^N \leq d_{2N+1}4^N \int_0^1 f dx \leq d_{2N+1}$. Apply log on both ends, and use (a) to conclude

$$2N \log 2 \leq \log(2N+1) \cdot \pi(2N+1).$$

3. Fix $x = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, where the p_i's are pairwise distinct. Recall that

$$\phi(x) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \ldots (p_r - 1)p_r^{\alpha_r - 1}.$$

From this formula it follows that $\phi(x) \geq p_i - 1$ for all i. Therefore, no prime greater than $\phi(x) + 1$ can divide x. Indeed, no prime power greater than $2\phi(x)$ can divide x, as $2\phi(x) \geq 2(p_i - 1)p_i^{\alpha_i - 1} \geq p_i^{\alpha_i}$ for all i. Therefore if $\phi(x) = n$ for a fixed n, then there are only finitely prime powers that could possibly divide x. This shows that the number of x that satisfies $\phi(x) = n$ is finite.

Next, we are asked to list all x with $\phi(x) = 100$. In doing this, it is much easier to consider the divisors of n (which we know well) than the possible divisors of x (which are prime powers less than or equal to 200, which are too numerous and irregular) like we did earlier. So we start by finding the prime powers whose value under ϕ is a divisor of 100. The divisors of 100 are 1, 2, 4, 5, 10, 20, 25, 50, 100, and

$\phi(p^\alpha) = (p-1)(p^{\alpha-1}) = 1$ has one solution $(p, \alpha) = (2, 1)$.

$(p-1)(p^{\alpha-1}) = 2$ has solutions $(2,2)$ and $(3,1)$.

$(p-1)(p^{\alpha-1}) = 4$ has solutions $(2,3)$ and $(5,1)$.

$(p-1)(p^{\alpha-1}) = 5$ has no solutions.

$(p-1)(p^{\alpha-1}) = 10$ has a solution $(11,1)$.

$(p-1)(p^{\alpha-1}) = 20$ has a solution $(5,2)$.

$(p-1)(p^{\alpha-1}) = 25$ has no solutions.

$(p-1)(p^{\alpha-1}) = 50$ has no solutions.

$(p-1)(p^{\alpha-1}) = 100$ has solutions $(5,3)$ and $(101,1)$.

Given this list, it is easy to see that the solutions to $\phi(x) = 100$ are precisely 101, $5^3 = 125$, $2 \cdot 101 = 202$, and $2 \cdot 5^3 = 250$.

4. First of all, note that $1+2+3+\ldots+(p-1) = p(p-1)/2$ by the summation formula. Wilson's theorem implies that $(p-1)! = (p-1) + Cp$ for some $C \in \mathbb{N}$. From this equation we see that $p-1 \mid C$. Since $(p-1)p$ is always even, we may write $Cp = C'p(p-1)/2$ for some $C \in \mathbb{N}$. Therefore,

$$(p-1)! = (p-1) + C' \cdot \frac{p(p-1)}{2}.$$

This completes the proof.

Alternative proof: This time we use the Chinese remainder theorem. $(p-1)! \equiv p-1 \pmod{p}$ by Wilson's theorem and $(p-1)! \equiv 0 \pmod{(p-1)/2}$. Since p and $(p-1)/2$ are coprime, there exists a unique number between 1 and $p(p-1)/2$ that is $p-1$ mod p and 0 mod $(p-1)/2$, namely $p-1$. Therefore $(p-1)! \equiv p-1 \pmod{p(p-1)/2}$.

5. $(1+a+a^2+\ldots+a^{p-2})(a-1) = a^{p-1}-1$. By Fermat's little theorem, $p \mid a^{p-1}-1$. But since $p \nmid a-1$ by assumption, $p \mid 1+a+a^2+\ldots+a^{p-2}$.

6. Write $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Then for any $t \in \mathbb{Z}$, $f(x+tm) = a_n(x+tm)^n + \ldots + a_1(x+tm) + a_0$. By the binomial theorem, for any nonnegative integer d, we have $(x+tm)^d = x^d + C \cdot m \equiv x^d \pmod{m}$. (Of course here C is an integer.) Therefore $f(x) \equiv f(x+tm) \pmod{m}$.

Suppose $f(a) = p$ or $-p$. Then $f(a) \equiv 0 \pmod{p}$, and by the above result, $f(a+tm) \equiv 0 \pmod{p}$. So either $f(a+tm) = \pm p$ is prime or $f(a+tm)$ is zero or composite. Now, if $f(x)$ were prime for every $x \in \mathbb{Z}$, then either $f(a+tm)-p$ or $f(a+tm)+p$ has infinitely many roots for t; i.e. $f(x)-p=0$ or $f(x)+p=0$ has infinitely many roots. But then it is impossible for any nonconstant polynomial to have infinitely many roots.