Fall 2021 – Math 328K – 55385

Homework 10 Solutions

Problem 1. Let $m, k \in \mathbb{Z}_+$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Show that

$$\operatorname{ord}(a^k) = \frac{\operatorname{ord}(a)}{(\operatorname{ord}(a), k)}.$$

Solution 1. To simplify notation, write $s = \operatorname{ord}(a)$ and $t = \operatorname{ord}(a^k)$. Then $(a^k)^{s/(s,k)} = (a^s)^{k/(s,k)} = [1]$, so $t \leq \frac{s}{(s,k)}$.

Assume that $t < \frac{s}{(s,k)}$. Then $kt < \frac{ks}{(s,k)} = \operatorname{lcm}(s,k)$, so kt is not a common multiple of s and k. It is clearly a multiple of k though, so $s \nmid kt$. This means that $kt = qs + r$ for some integers q and r with $0 < r < s$. But $a^r = a^{kt-qs} = (a^k)^t(a^s)^{-q} = [1]$, a contradiction to s being the least exponent n with $a^n = [1]$. So $t = \frac{s}{(s,k)}$.

Problem 2. Let $m \in \mathbb{Z}_+$ be a positive integer such that $\mathbb{Z}/m\mathbb{Z}$ has a primitive root. Show the following generalization of Wilson's Theorem:

$$\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x = -1.$$

Solution 2. Assume $m \neq 2$ and let $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ be a primitive root. First note that $[-1]$ is the unique $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $\operatorname{ord}(x) = 2$. This is since every such x can be written as r^k for some $k \in \{0, \ldots, \phi(m) - 1\}$ and by Problem 1

$$\operatorname{ord}(x) = \operatorname{ord}(r^k) = \frac{\operatorname{ord}(r)}{(\operatorname{ord}(r), k)} = \frac{\phi(m)}{(\phi(m), k)},$$

so $\operatorname{ord}(x) = 2$ if and only if $\frac{\phi(m)}{2} = (\phi(m), k)$. Clearly this is only the case for a single k, namely $k = \phi(m)/2$. So $[-1] = r^{\phi(m)/2}$, and this is the unique element of $(\mathbb{Z}/m\mathbb{Z})^\times$ with order 2.

Now

$$\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x = \prod_{k \in \mathbb{Z}/\phi(m)\mathbb{Z}} r^k = r^{\sum_{k \in \mathbb{Z}/\phi(m)\mathbb{Z}} k}.$$

In the sum over all elements $k \in \mathbb{Z}/\phi(m)\mathbb{Z}$, every k cancels out with $-k$ unless $k = -k$. Since $\phi(m)$ is even, there are exactly two such k, namely $[0]_{\phi(m)}$ and $[\phi(m)/2]_{\phi(m)}$. So

$$\sum_{k \in \mathbb{Z}/\phi(m)\mathbb{Z}} k = \left[\frac{\phi(m)}{2}\right]_{\phi(m)}$$

and therefore $\prod_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x = r^{\phi(m)/2} = [-1]_m$.

If $m = 2$, then $\prod_{x \in (\mathbb{Z}/2\mathbb{Z})^\times} x = [1]_2 = [-1]_2$.

Problem 3.

a) Let p be an odd prime. Show that the equation $x^4 = -1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ if and only if

$$p \bmod 8 = 1 \bmod 8,$$

and has exactly 4 solutions in that case.

b) Let $m \in \mathbb{Z}_+$ and write $m = 2^{i_0} p_1^{i_1} \cdots p_k^{i_k}$ for distinct odd primes $p_1, \ldots, p_k$, $i_0 \geq 0$, and $i_1, \ldots, i_k \geq 1$. Show the equation $x^4 = -1$ has a solution in $\mathbb{Z}/m\mathbb{Z}$ if and only if

$$i_0 \in \{0, 1\} \quad \text{and} \quad p_j \bmod 8 = 1 \bmod 8 \quad \text{for all } j \in \{1, \ldots, k\},$$

and has exactly 4^k solutions in that case.

Solution 3.

a) First note that [0] is not a solution, so we can restrict our attention to $(\mathbb{Z}/p\mathbb{Z})^\times$.

Let $r \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root. We can write every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ as r^k for a unique $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. For example, $r^k = [-1]$ iff $k = [\frac{p-1}{2}]$. So $(r^k)^4 = [-1]$ if and only if $4k = [\frac{p-1}{2}]$. Recall that this linear Diophantine equation has a solution in $\mathbb{Z}/(p-1)\mathbb{Z}$ if and only if $(4, p-1) \mid \frac{p-1}{2}$, and has $(4, p-1)$ solutions in this case.

Write $p - 1 = 2^i m$ with $i, m \geq 0$ and m odd. Then in fact $i \geq 1$ as otherwise $p - 1$ would be odd, but we assumed $p \neq 2$. If $i = 1$, then $(4, p-1) = 2$ and $\frac{p-1}{2} = m$ is odd, so $(4, p-1) \nmid \frac{p-1}{2}$. If $i = 2$, then $(4, p-1) = 4$ and $\frac{p-1}{2} = 2m$, so again $(4, p-1) \nmid \frac{p-1}{2}$. If $i \geq 3$, then $(4, p-1) = 4$ and $\frac{p-1}{2} = 2^{i-1}m$, so $(4, p-1) \mid \frac{p-1}{2}$. So the equation $x^4 = [-1]$ has a solution if and only if $8 \mid p - 1$, and it has 4 solutions in that case.

b) Let $f(x) = x^4 + 1$. Then $f'(x) = 4x^3$. In the case that $m = p^k$ is a power of an odd prime p, by part a) we have no solutions unless $p \bmod 8 = 1 \bmod 8$, and in that case there are 4 solutions in $\mathbb{Z}/p\mathbb{Z}$. Let x be one of them. We noted before that $x \neq [0]_p$, so $f'(x) = 4x^3 \neq [0]_p$ ($[4]_p \neq [0]_p$). So Hensel's Lemma tells us that a unique lift of every solution in $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p^k\mathbb{Z}$ is a solution, in particular that we have exactly 4 solutions in $\mathbb{Z}/p^k\mathbb{Z}$.

Now assume that $m = 2^k$ is a power of two. Since the equation $x^4 = -1$ has no solutions in $\mathbb{Z}/4\mathbb{Z}$, it also has no solutions in $\mathbb{Z}/2^k\mathbb{Z}$ if $k \geq 2$. It has a unique solution in $\mathbb{Z}/2\mathbb{Z}$.

Write S_m for the number of solutions in $\mathbb{Z}/m\mathbb{Z}$. We showed that $S_2 = 1$, $S_{2^k} = 0$ for all $k \geq 2$, $S_{p^k} = 4$ for all odd primes p with $[p]_8 = [1]_8$ and $k \geq 1$, and $S_{p^k} = 0$ for all other primes p. If $m = 2^{i_0} p_1^{i_1} \cdots p_k^{i_k}$ as in the question, then by the Chinese Remainder Theorem

$$S_m = \begin{cases} S_{2^{i_0}} S_{p_1^{i_1}} \cdots S_{p_k^{i_k}} & \text{if } i_0 \geq 1, \\ S_{p_1^{i_1}} \cdots S_{p_k^{i_k}} & \text{if } i_0 = 0. \end{cases}$$

These products evaluate to 0 if any of the factors are 0, and to 4^k otherwise.

Problem 4. The n–th *Fermat number* is $F_n = 2^{2^n} + 1$ (the exponent is 2^n).

a) Show that $\operatorname{ord}_{F_n} 2 \leq 2^{n+1}$.

A remark on notation: for coprime $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$, the expressions $\operatorname{ord}_m a$, $\operatorname{ord}_m [a]_m$, *and* $\operatorname{ord} [a]_m$ *all mean the same thing, the order of* $[a]_m$ *in* $(\mathbb{Z}/m\mathbb{Z})^\times$.

b) Suppose p is a prime divisor of F_n, show that $\operatorname{ord}_p 2 = 2^{n+1}$.

Hint: first show that $\operatorname{ord}_p 2 \mid 2^{n+1}$ *to deduce that* $\operatorname{ord}_p 2$ *is a power of* 2 *and must divide* 2^n *if* $\operatorname{ord}_p 2 < 2^{n+1}$.

c) Use the previous part to show that $p = 2^{n+1}k + 1$ for some $k \in \mathbb{Z}_+$.

Solution 4.

a) We need to show that $[2]_{F_n}^{2^{n+1}} = [1]_{F_n}$, or equivalently $F_n \mid 2^{2^{n+1}} - 1$. But this follows from $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n(2^{2^n} - 1)$.

b) Recall that $\operatorname{ord}_m(x) \mid n$ if and only if $x^n = [1]$. So $\operatorname{ord}_p 2 \mid 2^{n+1}$ if and only if $[2]_p^{2^{n+1}} = [1]_p$, or equivalently $p \mid 2^{2^{n+1}} - 1$. We already showed that $F_n \mid 2^{2^{n+1}} - 1$, and $p \mid F_n$, so $\operatorname{ord}_p 2 \mid 2^{n+1}$.

All divisors of 2^{n+1} are powers of 2, so $\operatorname{ord}_p 2 = 2^k$ for some k. If $\operatorname{ord}_p 2 \neq 2^{n+1}$ then $k \leq n$, so $\operatorname{ord}_p 2 \mid 2^n$. As before, this is equivalent to $p \mid 2^{2^n} - 1$. But we also have $p \mid 2^{2^n} + 1$ by definition, so p divides the difference $(2^{2^n} + 1) - (2^{2^n} - 1) = 2$. So $p = 2$, which is impossible since F_n is odd. This shows that $\operatorname{ord}_p 2 = 2^{n+1}$.

c) We know that $\operatorname{ord}_p 2 \mid \phi(p)$, so $2^{n+1} \mid p - 1$. In other words, $p = 2^{n+1}k + 1$ for some $k \in \mathbb{Z}$, and $k \geq 1$ since $p > 1$.