Math 209-16 Homework 2

Due Date: Sep 27, 2022

P1.(1 pt) Show that if $p \equiv 3 \pmod 4$, then $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p$.

PROOF. For $i \in \mathbb{Z}$, $i \equiv (i-p) \equiv -(p-i) \pmod p$. Therefore, we have

$$\prod_{i=1}^{\frac{p-1}{2}} i \equiv \prod_{i=1}^{\frac{p-1}{2}} -(p-i) \equiv (-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} (p-i) \pmod p$$

Multiplying both sides by $\prod\limits_{i=1}^{\frac{p-1}{2}} i$, we get

$$(\prod_{i=1}^{\frac{p-1}{2}} i)^2 \equiv (-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i) \equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv 1 \pmod p$$

where we have used $p \equiv 3 \pmod 4$, and Wilson's theorem stating that $(p-1)! \equiv -1 (\text{mod } p)$. It follows that $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod p$. □

P2.(1 pt) What are the last two digits in the ordinary decimal representation of 3^{400}?

SOLUTION. From $3^{400} = 9^{200} = (10-1)^{200} = \sum_{i=0}^{200} \binom{200}{i} 10^i (-1)^{200-i}$, we see that

$$3^{400} \equiv \sum_{i=0}^{1} \binom{200}{i} 10^i (-1)^{200-i} \equiv 1 \pmod{100}$$

Thus, the last two digits are 01.

P3.(2 pts) Show that if p is prime then $\binom{p}{k} \equiv 0 \pmod p$ for $1 \leqslant k \leqslant p-1$.

PROOF. Since $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} \in \mathbb{Z}$ and the denominator $k!$ is not a multiple of p for $1 \leqslant k \leqslant p-1$, we have $p \mid \binom{p}{k}$, i.e., $\binom{p}{k} \equiv 0 \pmod p$. □

P4.(2 pts) For any prime p, if $a^p \equiv b^p \pmod{p}$, prove that $a^p \equiv b^p \pmod{p^2}$.

PROOF. By Fermat's little theorem, $a \equiv a^p \equiv b^p \equiv b(\text{mod } p)$, we have $a \equiv b(\text{mod } p)$. Write $a = pk + b$ for some $k \in \mathbb{Z}$. Then

$$a^p - b^p = (pk+b)^p - b^p = \sum_{i=1}^{p} \binom{p}{i} (pk)^i b^{p-i}$$

Therefore, $p^2 \mid (a^p - b^p)$, i.e., $a^p \equiv b^p \pmod{p^2}$. □

P5.(2 pts) If p is any prime other than 2 or 5, prove that p divides infinitely many of the integers $9, 99, 999, 9999, \cdots$. If p is any prime other than 2 or 5, prove that p divides infinitely many of the integers $1, 11, 111, 1111, \cdots$.

PROOF. We can write the first sequence $a_n = \overbrace{9 \cdots 9}^{n \text{ copies}} = 10^n - 1$. Since p is a prime other than 2 or 5, we have $(10, p) = 1$. By Fermat's little theorem, $10^{p-1} \equiv 1(\text{mod } p)$, i.e., $p \mid (10^{p-1} - 1) = a_{p-1}$. Moreover, $a_{p-1} \mid a_{(p-1)n}$, $\forall\, n \in \mathbb{N}$, so the first assertion follows. The second sequence is $b_n = \frac{a_n}{9}$. If $p \neq 3$, the conclusion can be deduced from the above. If $p = 3$, notice that $3 \mid b_n$ for any n that is divisible by 3. The proof is completed. □

P6.(2 pts) Let p be a prime number, and suppose that x is an integer such that $x^2 \equiv -2(\text{mod } p)$. By considering the numbers $u + xv$ for various pairs (u, v), show that at least one of the equations $a^2 + 2b^2 = p$, $a^2 + 2b^2 = 2p$ has a solution.

PROOF. Consider the set $S = \{u + xv \mid 0 \leqslant u, v \leqslant [\sqrt{p}];\ u, v \in \mathbb{Z}\}$. Since $\#S = ([\sqrt{p}] + 1)^2 > (\sqrt{p})^2 = p$, by the pigeonhole principle, there exist two elements $u_1 + xv_1$ and $u_2 + xv_2$ in S such that $u_1 + xv_1 \equiv u_2 + xv_2 \pmod{p}$. It follows that $u_1 - u_2 \equiv x(v_2 - v_1) \pmod{p}$, and hence we have the following

$$(u_1 - u_2)^2 \equiv x^2(v_1 - v_2)^2 \equiv -2(v_1 - v_2)^2 \pmod{p}$$

As a consequence, the positive integer $(u_1 - u_2)^2 + 2(v_1 - v_2)^2$, which by our choice of u and v is not greater than $([\sqrt{p}])^2 + 2([\sqrt{p}])^2$, must be a multiple of p. This gives us $(u_1 - u_2)^2 + 2(v_1 - v_2)^2 = p$ or $2p$. □

P7.(3 pts) Somebody incorrectly remembered Fermat's little theorem as saying that the congruence $a^{n+1} \equiv a (\text{mod } n)$ holds for all a if n is prime. Describe the set of positive integers n for which this property is in fact true. That is, determine all positive integers n such that $a^{n+1} \equiv a (\text{mod } n)$ for all $a \in \mathbb{Z}$.

Solution. Clearly $n = 1$ and 2 satisfy this condition, now we assume $n > 2$. First we claim that n must be square-free. Actually, if there is a prime p such that $p^2 \mid n$, taking $a = p$ will lead to a contradiction since $p^2 \mid a^{n+1}$ but $p^2 \nmid a$. Next we take $a = -1$, and we get $(-1)^{n+1} \equiv -1 \pmod n$, which means n has to be even. Now we write n as a product of distinct primes $n = p_1 \cdots p_k$, with $2 = p_1 < \cdots < p_k$ and $k > 1$. The condition $a^{n+1} \equiv a \pmod n$ boils down to $a(a^n - 1) \equiv 0 \pmod{p_i}$ for all a and all $i = 1, 2, \cdots, k$. Notice that this already holds for $i = 1$, i.e., $2 \mid a(a^n - 1)$ for all a. Next consider $i = 2$, which says $a(a^{2p_2 \cdots p_k} - 1) \equiv 0 \pmod{p_2}$. When $p_2 \nmid a$, we have $a^{2p_2 \cdots p_k} \equiv a^{2p_3 \cdots p_k} \pmod{p_2}$, if this is congruent to 1 for all a, it is necessary that $(p_2 - 1) \mid 2p_3 \cdots p_k$. But $p_3, \cdots, p_k$ are prime numbers larger than p_2, hence $\gcd(p_2 - 1, p_3 \cdots p_k) = 1$, and so $(p_2 - 1) \mid 2$, which forces p_2 to be 3. By the same argument, we can show that k cannot be larger than 4. Moreover, if $k = 3$ or 4, then $p_3 = 7$, and if $k = 4$, then $p_4 = 43$. Summing up, $1, 2, 6, 42, 1806$ are all the possibilities of n such that $a^{n+1} \equiv a \pmod n$ for all $a \in \mathbb{Z}$. $\square$

P8.(2 pts) Show that $\binom{p^\alpha}{k} \equiv 0 \pmod p$ for $0 < k < p^\alpha$.

Proof. Notice that $\binom{p^\alpha}{k} = \frac{p^\alpha}{k}\binom{p^\alpha - 1}{k-1}$. And since $0 < k < p^\alpha$, when k is factored as $k = p^\beta m$ with $(p, m) = 1$, we must have $\beta < \alpha$. Now, $\binom{p^\alpha}{k} = \frac{p^{\alpha-\beta}}{m}\binom{p^\alpha - 1}{k-1}$ being an integer, m should divide $p^{\alpha-\beta}\binom{p^\alpha-1}{k-1}$, and hence divides $\binom{p^\alpha-1}{k-1}$, as $(p, m) = 1$. Consequently, $p^{\alpha-\beta} | \binom{p^\alpha}{k}$, and in particular, $\binom{p^\alpha}{k} \equiv 0 \pmod p$. $\square$

P9.(3 pts) Show that $\binom{p^\alpha - 1}{k} \equiv (-1)^k \pmod p$ for $0 \leqslant k \leqslant p^\alpha - 1$.

Proof. We proceed by induction on k, where $0 \leqslant k \leqslant p^\alpha - 1$. This is true for $k = 0$. Now we assume that $\binom{p^\alpha-1}{n} \equiv (-1)^n \pmod p$ for $k = n$. For $k = n + 1$, we have

$$\binom{p^\alpha - 1}{n+1} + \binom{p^\alpha - 1}{n} = \binom{p^\alpha}{n+1} \overset{\textbf{P8}}{\equiv} 0 \ (\text{mod } p) \Longrightarrow \binom{p^\alpha - 1}{n+1} + (-1)^n \equiv 0 \ (\text{mod } p)$$

Thus, $\binom{p^\alpha-1}{n+1} \equiv (-1)^{n+1} \pmod p$, which completes the proof. $\square$

P10.(2 pts) Show that if r is a non-negative integer then all coefficients of the polynomial $(1+x)^{2^r} - (1+x^{2^r})$ are even. Write a positive integer n in binary, $n = \sum_{r\in\mathscr{R}} 2^r$. Show that all coefficients of the polynomial $(1+x)^n - \prod_{r\in\mathscr{R}}(1+x^{2^r})$ are even. Write $k = \sum_{s\in\mathscr{L}} 2^s$ in binary. Show that $\binom{n}{k}$ is odd if and only if $\mathscr{L} \subseteq \mathscr{R}$. Conclude that if n is given, then $\binom{n}{k}$ is odd for precisely $2^{w(n)}$ values of k, where $w(n)$, called the binary weight n, is the number of 1's in the binary expansion of n. In symbols, $w(n) = \mathrm{card}(\mathscr{R})$.

Proof. $(1+x)^{2^r} - (1+x^{2^r}) = \sum_{i=1}^{2^r-1}\binom{2^r}{i}x^i$, by Problem 8, $2 \mid \binom{2^r}{i}$ for $1 \leqslant i \leqslant 2^r - 1$, so the first assertion follows. For the second part, we have

$$\begin{aligned}
(1+x)^n - \prod_{r\in\mathscr{R}}(1+x^{2^r}) &= (1+x)^{\sum_{r\in\mathscr{R}} 2^r} - \prod_{r\in\mathscr{R}}(1+x^{2^r}) \\
&= \prod_{r\in\mathscr{R}}(1+x)^{2^r} - \prod_{r\in\mathscr{R}}(1+x^{2^r}) \\
&= \prod_{r\in\mathscr{R}}\left((1+x^{2^r}) + \sum_{i=1}^{2^r-1}\binom{2^r}{i}x^i\right) - \prod_{r\in\mathscr{R}}(1+x^{2^r})
\end{aligned}$$

Consider this polynomial modulo 2 (namely, in the ring $\mathbb{F}_2[x]$), we get

$$\prod_{r\in\mathscr{R}}\left((1+x^{2^r}) + \sum_{i=1}^{2^r-1}\binom{2^r}{i}x^i\right) - \prod_{r\in\mathscr{R}}(1+x^{2^r}) \equiv \prod_{r\in\mathscr{R}}((1+x^{2^r})+0) - \prod_{r\in\mathscr{R}}(1+x^{2^r}) \equiv 0 \pmod 2$$

Thus, all coefficients of the polynomial $(1+x)^n - \prod_{r\in\mathscr{R}}(1+x^{2^r})$ are even $(*)$.

$$\begin{aligned}
[x^k](1+x)^n = \binom{n}{k} \text{ is odd } &\iff [x^k]\left((1+x)^n - \prod_{r\in\mathscr{R}}(1+x^{2^r}) + \prod_{r\in\mathscr{R}}(1+x^{2^r})\right) \text{ is odd} \\
&\overset{(*)}{\iff} [x^k]\prod_{r\in\mathscr{R}}(1+x^{2^r}) \text{ is odd}
\end{aligned}$$

Notice that

$$\prod_{r\in\mathscr{R}}(1+x^{2^r}) = \sum_{\mathscr{R}_m\subseteq\mathscr{R}} x^m$$

where $m = \sum\limits_{i\in\mathscr{R}_m} 2^i$. Therefore, $[x^k]\prod_{r\in\mathscr{R}}(1+x^{2^r}) = \begin{cases} 1, & \text{if } \mathscr{L}\subseteq\mathscr{R}, \\ 0, & \text{otherwise.}\end{cases}$ and $\binom{n}{k}$ is odd if and only if $\mathscr{L}\subseteq\mathscr{R}$. Finally, since there are totally $2^{\mathrm{card}(\mathscr{R})} = 2^{w(n)}$ such subsets $\mathscr{L}\subseteq\mathscr{R}$, we conclude that there are exactly $2^{w(n)}$ values of k such that $\binom{n}{k}$ is odd. $\square$