Math 209-16 Homework 5

Due Date: Nov. 29 (Tue), 2022

P1.(2 pts) For any positive integers a, b, n, prove that if n is a divisor of $a^n - b^n$, then n is a divisor of $(a^n - b^n)/(a - b)$.

Proof. Obviously, it holds for $n = 1$, so we suppose that $n \geqslant 2$. Let $d = \gcd(a-b, n)$, and write the prime factorization of n as $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$. Note that it suffices to show $p_i^{n_i} \mid \frac{a^n-b^n}{a-b}$ for all i. We consider two cases as follows:

① If $p_i \nmid d$, then $p_i^{n_i} \mid \frac{a^n-b^n}{a-b}$ since $n \mid (a^n - b^n)$.

② If $p_i \mid d$, we claim that $p_i \mid a$ and $p_i \mid b$. Clearly, $p_i \mid (a - b)$, so we may write $a = b + kp_i$ for some $k \in \mathbb{Z}$, or equivalently, $a \equiv b \pmod{p_i}$. Thus, we have

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv nb^{n-1} \equiv 0 \pmod{p_i} \tag{1}$$

On the other hand, plug in $a = b + kp_i$, we get

$$\frac{a^n - b^n}{a - b} = \frac{(b + kp_i)^n - b^n}{kp_i} = \sum_{j=0}^{n-1} (kp_i)^j b^{n-j-1}$$

Together with (1), we see that $p_i \mid b$, and $p_i \mid a$ also follows. The claim is proved now. Next, we may write $a = p_i^{v_a} \cdots$ and $b = p_i^{v_b} \cdots$, namely, $v_a = v_{p_i}(a)$ and $v_b = v_{p_i}(b)$. Without loss of generality, we can assume that $v_a \geqslant v_b$. Then it follows that

$$v_{p_i}\left(\frac{a^n - b^n}{a - b}\right) = v_{p_i}(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}) \geqslant v_b \cdot (n - 1) \geqslant n - 1 \geqslant n_i,$$

which means that $p_i^{n_i} \mid \frac{a^n-b^n}{a-b}$. So we conclude that $n \mid (a^n - b^n) \Longrightarrow n \mid \frac{a^n-b^n}{a-b}$. $\square$

P2.(2 pts) Write n in base p, and let $S(n)$ denote the sum of the digits in this representation. Show that $p^e \parallel n!$, where $e = (n - S(n))/(p-1)$.

Proof 1. Suppose that $n = \sum_{i=0}^{k} a_i \cdot p^i$ with $k \geqslant 0$ and $a_i \in \{0, 1, \dots, p-1\}$, then $S(n) = \sum_{i=0}^{k} a_i$. Hence, we have

$$e = \sum_{i=1}^{k} [\frac{n}{p^i}] = \sum_{i=1}^{k} \sum_{j=i}^{k} a_j \cdot p^{j-i} = \sum_{j=1}^{k} a_j (\sum_{i=0}^{j-1} p^i) = \frac{\sum_{j=0}^{k} a_j (p^j - 1)}{p-1} = \frac{n - S(n)}{p-1}$$

□

Proof 2.[1] For each natural number m, if $v_p(m) = e$, then the base p expansion of m should be of the form $m = \sum_{i=e}^{k} a_i p^i$, with $k \geqslant i$, $0 \leqslant a_i \leqslant p-1$, and $a_e \neq 0$. Therefore the base p expansion of $m-1$ should be

$$m - 1 = \sum_{i=0}^{e-1} (p-1) p^i + (a_e - 1) p^e + \sum_{i=e+1}^{k} a_i p^i,$$

and we see immediately that $S(m-1) = (p-1)e + S(m) - 1$, in other words,

$$v_p(m) = e = \frac{1 + S(m-1) - S(m)}{p-1}.$$

As a consequence, we have

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \frac{1 + S(m-1) - S(m)}{p-1} = \frac{n - S(n)}{p-1}.$$

□

[1] We thank Prof. Qing Xiang for providing this proof.

P3.(2 pts) Let a and b be positive integers with $a+b=n$. Show that the power of p dividing $\binom{n}{a}$ is exactly the number of carries when a and b are added base p.

Proof. Notice that each time a carry happens when a and b are added in base p, the difference $S(a)+S(b)-S(n)$ would decrease by $p-1$. If no carry happens, then $S(a)+S(b)-S(n)=0$. Therefore, the number of such carries is equal to

$$\frac{S(a)+S(b)-S(n)}{p-1}=\frac{n-S(n)-(a-S(a))-(b-S(b))}{p-1}=e_n-e_a-e_b,$$

which is exactly the power of p dividing $\binom{n}{a}=\frac{n!}{a!b!}$. $\square$

P4.(2 pts) Suppose that $a=\alpha p+a_0$ and that $0\leqslant a_0<p$. Show that $a!/(\alpha!p^\alpha)\equiv(-1)^\alpha a_0! \pmod p$. Suppose also that $b=\beta p+b_0$ with $0\leqslant b_0<p$. Show that $\binom{a+b}{a}\equiv\binom{\alpha+\beta}{\alpha}\binom{a_0+b_0}{a_0} \pmod p$. Deduce that if $a=\sum_i a_ip^i$ and $b=\sum_i b_ip^i$ in base p, then $\binom{a+b}{a}\equiv\prod_i\binom{a_i+b_i}{a_i} \pmod p$.

Proof. When $a_0\geqslant 1$, we have the following:

$$\frac{a!}{\alpha!p^\alpha}=\prod_{k=1}^{a_0}(\alpha p+k)\cdot\frac{(\alpha p)!}{\alpha!p^\alpha}=\prod_{k=1}^{a_0}(\alpha p+k)\cdot\prod_{i=0}^{\alpha-1}\prod_{j=1}^{p-1}(ip+j)\equiv a_0!\cdot((p-1)!)^\alpha\equiv(-1)^\alpha a_0! \pmod p,$$

where the second equality holds because all the multiples of p appearing in the numerator are cancelled out by the denominator. In the case of $a_0=0$, the result is consistent with above since the term $\prod_{k=1}^{a_0}(\alpha p+k)$ disappears and $a_0!=0!=1$. Hence, the first congruence follows. This leads to the second congruence:

$$\begin{aligned}\binom{a+b}{a}&=\frac{(a+b)!}{a!b!}=\frac{\frac{(a+b)!}{(\alpha+\beta)!p^{\alpha+\beta}}}{\frac{a!}{\alpha!p^\alpha}\cdot\frac{b!}{\beta!p^\beta}}\cdot\binom{\alpha+\beta}{\alpha}\equiv\frac{\frac{(a+b)!}{(\alpha+\beta)!p^{\alpha+\beta}}}{\frac{a!}{\alpha!p^\alpha}\cdot\frac{b!}{\beta!p^\beta}}\cdot\binom{\alpha+\beta}{\alpha}\cdot\frac{\frac{a!}{\alpha!p^\alpha}}{(-1)^\alpha a_0!}\cdot\frac{\frac{b!}{\beta!p^\beta}}{(-1)^\beta b_0!}\\&\equiv\frac{(-1)^{\alpha+\beta}(a_0+b_0)!}{(-1)^\alpha a_0!(-1)^\beta b_0!}\cdot\binom{\alpha+\beta}{\alpha}=\binom{\alpha+\beta}{\alpha}\binom{a_0+b_0}{a_0} \pmod p.\end{aligned}$$

where we have used $\frac{\frac{a!}{\alpha!p^\alpha}}{(-1)^\alpha a_0!}\equiv 1 \pmod p$. Also notice that even if $a_0+b_0\geqslant p$, $\frac{(a+b)!}{(\alpha+\beta)!p^{\alpha+\beta}}\equiv(-1)^{\alpha+\beta}(a_0+b_0)! \pmod p$ still holds since in this case both sides are divisible by p. Finally, the last congruence is an immediate consequence by induction of the previous one. $\square$

P5.(2 pts) Show that the sum of the odd divisors of n is $-\sum_{d|n}(-1)^{n/d}d$, and that this is $\sigma(n)-2\sigma(n/2)$ where $\sigma(a)$ is defined to be 0 if a is not an integer.

Proof. To prove the first identity, we write $n = 2^t \cdot l$ with l odd. Then

$$-\sum_{d|n}(-1)^{n/d}d = -\sum_{i=0}^{t}\sum_{k|l}(-1)^{2^{t-i}\cdot\frac{l}{k}}2^i k = 2^t\sum_{k|l}k - \left(\sum_{i=0}^{t-1}2^i\right)\sum_{k|l}k = \sum_{k|l}k,$$

which is exactly the sum of odd divisors of n.

It is also easy to see that the sum of odd divisors of n is equal to $\sigma(n)-2\sigma(n/2)$. Indeed, if n is odd, they are both equal to $\sigma(n)$ since all the divisors of n are odd. And if $n = 2m$ is even, the even divisors of n are exactly those of the form $2d$ with $d|m$, therefore, the sum of even divisors of n is $\sum_{d|m}2d = 2\sigma(m) = 2\sigma(n/2)$. □

P6.(2 pts) Show that for all positive integers n,

$$\sum_{\substack{a=1\\(a,n)=1}}^{n}(a-1,n) = d(n)\phi(n).$$

Proof. For $n = p^k$ a prime power, by direct computations we see that

$$\sum_{\substack{a=1\\(a,p)=1}}^{p^k}(a-1,p^k) = (p^k-2p^{k-1}) + \sum_{i=1}^{k-1}p^i(p^{k-i}-p^{k-i-1}) + p^k = (k+1)p^{k-1}(p-1) = d(n)\phi(n),$$

where p^k-2p^{k-1} is the sum of those terms with $(a-1,p^k)=1$, $p^i(p^{k-i}-p^{k-i-1})$ is the sum of those terms with $(a-1,p^k)=p^i$, and p^k represents the first term with $(1-1,n)=p^k$.

Now it suffices to show that both sides of the identity are multiplicative functions of n. Since $d(n)$ and $\phi(n)$ are well-known to be multiplicative, we are only left to consider the LHS. Suppose that $(m,n)=1$, then $an+bm$ runs over a reduced residue system modulo mn if a (resp. b) runs over a reduced residue system modulo m (resp. n).

Therefore, we have

$$\begin{aligned}
\sum_{\substack{c=1\\(c,mn)=1}}^{mn} (c-1, mn) &= \sum_{\substack{a=1\\(a,m)=1}}^{m} \sum_{\substack{b=1\\(b,n)=1}}^{n} (an+bm-1, mn) \\
&= \sum_{\substack{a=1\\(a,m)=1}}^{m} \sum_{\substack{b=1\\(b,n)=1}}^{n} (an+bm-1, m)(an+bm-1, n) \\
&= \sum_{\substack{a=1\\(a,m)=1}}^{m} \sum_{\substack{b=1\\(b,n)=1}}^{n} (an-1, m)(bm-1, n) \\
&= \left(\sum_{\substack{a=1\\(a,m)=1}}^{m} (an-1, m) \right) \left(\sum_{\substack{b=1\\(b,n)=1}}^{n} (bm-1, n) \right) \\
&= \left(\sum_{\substack{a=1\\(a,m)=1}}^{m} (a-1, m) \right) \left(\sum_{\substack{b=1\\(b,n)=1}}^{n} (b-1, n) \right)
\end{aligned}$$

where in the last step we have used the fact that when a runs over a reduced residue system of $\pmod{m}$, so does an, and similar for b. $\square$

P7.(2 pts) Let $s(n)$ denote the largest square-free divisor of n. That is, $s(n) = \prod_{p|n} p$. Show that $\sum_{d|n} d\mu(d) = (-1)^{\omega(n)}\phi(n)s(n)/n$.

Proof. Let $n = p_1^{t_1} \cdots p_k^{t_k}$ be its prime factorization. Then

$$\sum_{d|n} d\mu(d) = \sum_{s=0}^{k} (-1)^s \sum_{1 \leqslant i_1 < \cdots < i_s \leqslant k} p_{i_1} \cdots p_{i_s} = \prod_{i=1}^{k}(1-p_i) = (-1)^{\omega(n)} \prod_{i=1}^{k}(p_i - 1),$$

while it is easy to see that $\phi(n)s(n)/n = \prod_{i=1}^{k}(p_i - 1)$. Combining the two equalities, the proof is now completed. $\square$

P8.(2 pts) Let $\Phi_n(x)$ denote the polynomial with leading coefficient 1 and degree $\phi(n)$ whose roots are the $\phi(n)$ different primitive n-th roots of unity. Prove that $\prod_{d|n} \Phi_d(x) = x^n - 1$ for all real or complex numbers x. Deduce that $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$. Show that the coefficients of $\Phi_n(x)$ are integers. This is the *cyclotomic polynomial* of order n.

Proof. The polynomial $x^n - 1$ can be factored as $\prod_\zeta (x - \zeta)$ where ζ runs over all the n-th roots of unity. Now any n-th root of unity is a primitive d-th root of unity for precisely one $d \mid n$ and conversely, any primitive d-th root of unity with $d \mid n$ is of course an n-th root of unity. Therefore, we have the factorization $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Then it follows from Möbius inversion (see Problem 23 on Page 197 of the textbook) that $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$. To show that the coefficients of $\Phi_n(x)$ are integers, we proceed by induction on n. Clearly, it is true for $\Phi_1(x) = x - 1$, and now we assume that the conclusion holds for all integers less than n. Then $\prod_{d|n, d<n} \Phi_d(x)$ is a monic polynomial with coefficients in $\mathbb{Z}$, and we see from $\prod_{d|n} \Phi_d(x) = x^n - 1$ that it divides $x^n - 1$ over $\mathbb{C}$, and hence over $\mathbb{Q}$ since $\prod_{d|n,d<n} \Phi_d(x)$ is monic. As a consequence, $\Phi_n(x)$ has coefficients in $\mathbb{Q}$. Hence, by Gauss's lemma we see that the coefficients of $\Phi_n(x)$ are integers. $\square$

P9.(2 pts) Let p be prime, and let $\Phi_{p-1}(x)$ denote the cyclotomic polynomial of order $p-1$. Show that g is a solution of the congruence $\Phi_{p-1}(x) \equiv 0 \pmod{p}$ if and only if g is a primitive root $\pmod{p}$. Show also that the sum of all the primitive roots $\pmod{p}$ is $\equiv \mu(p-1) \pmod{p}$.

Proof. If g is a primitive root $\pmod{p}$, then g is a root of $x^{p-1} - 1 \pmod{p}$ but not a root of $x^d - 1 \pmod{p}$ for any $d < p - 1$. In particular, since $\Phi_d(x)$ is a factor of $x^d - 1$, g cannot be a root of $\Phi_d(x) \pmod{p}$ for $d < p - 1$. Therefore g must be a root of $\phi_{p-1}(x) \pmod{p}$ as $\prod_{d|p-1} \Phi_d(x) = x^{p-1} - 1$. Since there are exactly $\phi(p-1)$ primitive roots $\pmod{p}$, and there are at most $\deg(\Phi_{p-1}(x)) = \phi(p-1)$ different roots of $\Phi_{p-1}(x) \pmod{p}$, we deduce that g is a solution of the congruence $\Phi_{p-1}(x) \equiv 0 \pmod{p}$ if and only if g is a primitive root $\pmod{p}$. Let ζ be a primitive root modulo p, i.e., $\mathbb{Z}_p^\times = \langle \zeta \rangle$. Then the sum of all the primitive roots $\pmod{p}$ is $\sum_{k=1,(k,p-1)=1}^{p-1} \zeta^k$. Since $\sum_{d|n} \mu(d) = 1$ if $n = 1$; otherwise, it is 0, we have

$$\sum_{k=1,(k,p-1)=1}^{p-1} \zeta^k = \sum_{k=1}^{p-1} \zeta^k \sum_{d|(k,p-1)} \mu(d) = \sum_{d|(p-1)} \mu(d) \sum_{j=1}^{\frac{p-1}{d}} \zeta^{jd} \equiv \mu(p-1) \pmod{p}. \quad \square$$

P10.(2 pts) Let p be a prime number. Show that $F_p \equiv (\frac{p}{5}) \pmod{p}$. Show that $F_{p+1} \equiv 1 \pmod{p}$ if $p \equiv \pm 1 \pmod{5}$, and that $F_{p+1} \equiv 0 \pmod{p}$ if $p \equiv \pm 2 \pmod{5}$. Show that $F_{p-1} \equiv 0 \pmod{p}$ if $p \equiv \pm 1 \pmod{5}$, and that $F_{p-1} \equiv 1 \pmod{p}$ if $p \equiv \pm 2 \pmod{5}$. Conclude that if $p \equiv \pm 1 \pmod{5}$ then $p-1$ is a period of $F_n \pmod{p}$. (This is not necessarily the least period.) Conclude also that if $p \equiv \pm 2 \pmod{5}$ then $2p+2$ is a period of $F_n \pmod{p}$.

Proof. Recall $F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$ for $n = 0, 1, \cdots$. Therefore, we have

$$\begin{aligned} F_p &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^p - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^p \equiv \frac{1}{2\sqrt{5}}(1 + 5^{p/2} - 1 + 5^{p/2}) \\ &= 5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \pmod{p}. \end{aligned}$$

Similarly,

$$\begin{aligned} F_{p+1} &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{p+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{p+1} \\ &\equiv \frac{1}{4\sqrt{5}}\left((1+5^{p/2})(1+5^{1/2}) - (1-5^{p/2})(1-5^{1/2})\right) \\ &= \frac{5^{\frac{p-1}{2}}+1}{2} \\ &\equiv \frac{\left(\frac{5}{p}\right)+1}{2} = \frac{\left(\frac{p}{5}\right)+1}{2} \pmod{p}. \end{aligned}$$

Since

$$\left(\frac{p}{5}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{5} \\ -1, & p \equiv \pm 2 \pmod{5} \end{cases}$$

the above result is exactly what we want. Moreover, the result on F_{p-1} follows immediately from $F_{p-1} = F_{p+1} - F_p$.

Finally, if $p \equiv \pm 1 \pmod{5}$, we see that $F_p \equiv 1 = F_1 \pmod{p}$ and $F_{p+1} \equiv 1 = F_2 \pmod{p}$, hence $p-1$ is a period of $F_n \pmod{p}$. While if $p \equiv \pm 2 \pmod{5}$, then $F_{p+1} \equiv 0 = -F_0 \pmod{p}$ and $F_{p+2} = F_{p+1} + F_p \equiv -1 = -F_1 \pmod{p}$, hence $F_{n+p+1} \equiv -F_n \pmod{p}$ and so $F_{n+2p+2} \equiv F_n \pmod{p}$ for any n. $\square$