Math 40520 Theory of Number
Homework 9

Due Wednesday, 2015-12-02, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. Let p be a prime and $k, n \geq 1$ integers. Show that

$$v_p((p^k n)!) = \frac{n(p^k - 1)}{p - 1} + v_p(n!)$$

Proof. Write $n = \overline{n_d \dots n_1 n_0}_{(p)}$. Then $np^k = \overline{n_d \dots n_1 n_0 \underbrace{0 \dots 0}_{k}}$. Applying our formula we get

$$v_p((p^k n)!) = \frac{p^k n - \sum n_i}{p - 1}$$

and

$$v_p(n!) = \frac{n - \sum n_i}{p - 1}$$

Immediately we get

$$v_p((p^k n)!) = \frac{p^k n - (n - (p-1)v_p(n!))}{p - 1} = \frac{n(p^k - 1)}{p - 1} + v_p(n!)$$

□

2. Let p be a prime.

   (a) For an integer n write $n = pq + r$ where $0 \leq r \leq p - 1$. Show that

$$\prod_{1 \leq d \leq n, (d,p)=1} d \equiv (-1)^q r! \pmod{p}$$

   [Hint: Wilson's theorem.]

   (b) Write $n = \overline{n_d \dots n_1 n_0}_{(p)}$ and $\ell = v_p(n!)$. Conclude that

$$\frac{n!}{p^\ell} \equiv (-1)^\ell n_0! n_1! \cdots n_d! \pmod{p}$$

Proof. (a) Note that

$$\prod_{\ell p + 1 \leq d \leq (\ell+1)p, (d,p)=1} d \equiv \prod_{1 \leq d \leq p, (d,p)=1} d \equiv (p-1)! \equiv -1 \pmod{p}$$

and so

$$\begin{aligned}\prod_{1\le d\le n,(d,p)=1} d &= \prod_{\ell=0}^{q-1}\left(\prod_{\ell p+1\le d\le(\ell+1)p,(d,p)=1} d\right)\times\prod_{pq+1\le d\le n,(d,p)=1} d\\ &\equiv (-1)^q\prod_{1\le d\le r,(d,p)=1} d \pmod p\\ &\equiv (-1)^q r! \pmod p\end{aligned}$$

(b) Note that $\ell = v_p(n!) = \sum_{k=1}^n v_p(k)$ and so

$$\frac{n!}{p^\ell} = \prod_{k=1}^n \frac{k}{p^{v_p(k)}}$$

where the RHS can be rewritten not as k goes from 1 to n but as $v_p(k)$ goes from 1 on, as follows:

$$\frac{n!}{p^\ell} = \prod_{e\ge 0}\prod_{1\le k\le n, v_p(k)=e}\frac{k}{p^e}$$

Note that if $v_p(k) = e$ then $k = p^e d$ where $1 \le d \le n/p^e$ and $(d, e) = 1$. Thus we can further rewrite the product as

$$\frac{n!}{p^\ell} = \prod_{e\ge 0}\left(\prod_{1\le d\le\lfloor n/p^e\rfloor,(d,p)=1} d\right)$$

The first part tells us that the inner product is congruent mod p to $(-1)^q r!$ where $\lfloor n/p^e\rfloor = pq + r$. Writing $n = \overline{n_d \dots n_1 n_0}_{(p)}$ we see that $\lfloor n/p^e\rfloor = \overline{n_d \dots n_e}_{(p)} = p\cdot\overline{n_d \dots n_{e+1}}_{(p)} + n_e = p\lfloor n/p^{e+1}\rfloor + n_e$ so the inner product is congruent mod p to $(-1)^{\lfloor n/p^{e+1}\rfloor} n_e!$.

Thus

$$\begin{aligned}\frac{n!}{p^\ell} &\equiv \prod_{e\ge 0}(-1)^{\lfloor n/p^{e+1}\rfloor} n_e! \pmod p\\ &= (-1)^{\sum_{e\ge 0}\lfloor n/p^{e+1}\rfloor}\prod_{e\ge 0} n_e! \pmod p\\ &= (-1)^\ell\prod n_e! \pmod p\end{aligned}$$

because we know that $\ell = v_p(n!) = \sum_{e\ge 1}\lfloor n/p^e\rfloor$. □

3. Let p be a prime and m, n two integers. Write $m = \overline{m_d \dots m_1 m_0}_{(p)}$, $n = \overline{n_d \dots n_1 n_0}_{(p)}$ and $m - n = \overline{k_d \dots k_1 k_0}_{(p)}$. Show that if $\ell = v_p\left(\binom{m}{n}\right)$ then

$$p^{-\ell}\binom{m}{n} \equiv (-1)^\ell\prod_{i=0}^d\frac{m_i!}{n_i!k_i!} \pmod p$$

Proof. Let $\mu = v_p(m!)$, $\nu = v_p(n!)$ and $\kappa = v_p(k!)$ in which case $\ell = \mu - \nu - \kappa$. Thus

$$\begin{aligned}p^{-\ell}\binom{m}{n} &= \frac{p^{-\mu}m!}{p^{-\nu}n!\cdot p^{-\kappa}k!}\\ &\equiv \frac{(-1)^\mu\prod m_i!}{(-1)^\nu\prod n_i!\cdot(-1)^\kappa\prod k_i!}\\ &\equiv (-1)^\ell\prod\frac{m_i!}{n_i!k_i!} \pmod p\end{aligned}$$

using the previous problem. $\square$

4. (Variant of Exercise 8.3 on page 146) For a positive integer n and a complex number s define

$$\sigma_s(n) = \sum_{d|n} d^s$$

(a) Show that if m and n are coprime then $\sigma_s(mn) = \sigma_s(m)\sigma_s(n)$.

(b) Show that if $n = p_1^{k_1} \cdots p_r^{k_r}$ and $s \neq 0$ then

$$\sigma_s(n) = \prod_{i=1}^{r} \frac{p_i^{s(k_i+1)} - 1}{p_i^s - 1}$$

Proof. (a): Suppose $d \mid mn$ and write $a = (d, m)$. Then $d/a \mid mn/a$ and since $(d/a, m/a) = 1$ it follows that $b = d/a \mid n$ so d can be written as $d = ab$ with $a \mid m$ and $b \mid n$. Reciprocally, given $a \mid m$ and $b \mid n$ then clearly $d = ab \mid mn$. Thus

$$\sigma_s(mn) = \sum_{d|mn} d^s = \sum_{a|m} \sum_{b|n} (ab)^s = \sum_{a|m} a^s \sum_{b|n} b^s = \sigma_s(m)\sigma_s(n)$$

(b): We compute

$$\sigma_s(p^k) = 1^s + p^s + (p^2)^s + \cdots + (p^k)^s = 1 + p^s + (p^s)^2 + \cdots + (p^s)^k = \frac{p^{s(k+1)} - 1}{p^s - 1}$$

Using part (a)

$$\sigma_s(n) = \prod_{i=1}^{r} \sigma_s(p_i^{k_i}) = \prod_{i=1}^{r} \frac{p_i^{s(k_i+1)} - 1}{p_i^s - 1}$$

$\square$

5. Let $p \equiv 1 \pmod 3$ be a prime.

(a) Show that there exists $u \in \mathbb{Z}$ such that $u^2 + u + 1 \equiv 0 \pmod p$.

(b) Show that there exist integers x, y such that $p = x^2 + xy + y^2$. [Hint: What is the area of ellipse $x^2 + xy + y^2 = R^2$?]

Proof. (a): As $p \neq 2$ the equation is equivalent to $(2u + 1)^2 + 3 = 4(u^2 + u + 1) \equiv 0 \pmod p$ which clearly has a solution as $\left(\frac{-3}{p}\right) = 1$ if $p \equiv 1 \pmod 3$.

(b): As in class consider the lattice $L = \{(x, y) \in \mathbb{Z}^2 \mid y \equiv ux \pmod p\}$ and the centrally symmetric convex ellipse X whose boundary is given by the equation $x^2 + xy + y^2 = \alpha p$ where we'll choose the coefficient α later. The ellipse $x^2 + xy + y^2 = R^2$ has the axes along the $y = \pm x$ axes with long radius $\sqrt{2}R$ on the $y = -x$ line and short radius $\sqrt{2}R/\sqrt{3}$ on the $y = x$ line. Its area, from calculus, is $2\pi R^2/\sqrt{3}$. The area of X is then $2\pi\alpha p/\sqrt{3}$.

As in class the area of the fundamental parallelogrom of the lattice L is p and to apply Minkowski's theorem we require the area $2\pi\alpha p/\sqrt{3}$ of X to be $> 4p$ so we require $\alpha > 2\sqrt{3}/\pi \approx 1.1$. For example $\alpha < 2$ close to 2 will work. Then Minkowski guarantees $X \cap L$ contains a nonzero point (x, y). As $(x, y) \in L$ it follows that $x^2 + xy + y^2 \equiv x^2(u^2 + u + 1) \equiv 0 \pmod p$. As $(x, y) \in X$ it follows that $x^2 + xy + y^2 < \alpha p$ and the only integer in the range $(0, \alpha p) \subset (0, 2p)$ which is divisible by p is p itself. Thus $p = x^2 + xy + y^2$. $\square$

6. Exercise 8.24 on page 163.

Proof. Write $n = \prod p_i^{k_i}$. Then $d \mid n$ is a prime power if and only if $d \mid p_i^{k_i}$ for some i. In this case either $\Lambda(d) = 0$ if $d = 1$ or $\Lambda(d) = \ln(p_i)$ if $d \neq 1$.

Therefore

$$\sum_{d|n} \Lambda(d) = \sum_i \sum_{d|p_i^{k_i}} \Lambda(d) = \sum_i \sum_{e=1}^{k_i} \Lambda(p_i^e) = \sum_i k_i \ln(p_i) = \sum_i \ln(p_i^{k_i}) = \ln(n)$$

(b): Applying Mobius inversion we get

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln(n/d) = \ln(n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \ln(d) = -\sum_{d|n} \mu(d) \ln(d)$$

□

7. Exercise 8.21 on page 163.

Proof. (a): We need that $\chi(mn) = \chi(m)\chi(n)$ for all m, n. If one of m or n is even then this is trivial as $0 = 0 \cdot$ anything. If m and n are odd then note that $\chi(m) \equiv m \pmod 4$ so the χ is clearly multiplicative.

(b): Using part (a) note that for $u = 1$ or 3,

$$\begin{aligned} \tau_u(n) &= \#\{d \mid n \mid d \equiv u \pmod 4\} \\ &= \#\{d \mid n \mid \chi(d) \equiv u \pmod 4\} \\ &= \sum_{d|n, \chi(d) \equiv u \pmod 4} 1 \end{aligned}$$

and so we may compute

$$\begin{aligned} g(n) = \tau_1(n) - \tau_3(n) &= \sum_{d|n, \chi(d)=1} 1 - \sum_{d|n, \chi(d)=-1} 1 \\ &= \sum_{d|n, \chi(d)=1} \chi(d) + \sum_{d|n, \chi(d)=-1} \chi(d) \\ &= \sum_{d|n} \chi(d) \end{aligned}$$

which is then multiplicative as in class because χ is multiplicative.

Thus $g(n) = \prod g(p_i^{k_i})$. But $\sum_{e=0}^k 1 = k+1$ and $\sum_{e=0}^k (-1)^e = 0$ if k is odd and $= 1$ if k is even so

$$g(p^k) = \sum_{d|p^k} \chi(d) = \sum_{e=0}^k \chi(p)^k = \begin{cases} 0 & \chi(p) = 0 \\ k+1 & \chi(p) = 1 \\ 0 \text{ or } 1 & \chi(p) = -1 \end{cases} = \begin{cases} 0 & p = 2 \\ k+1 & p \equiv 1 \pmod 4 \\ 0 \text{ or } 1 & p \equiv 3 \pmod 4 \end{cases}$$

Writing $n = 2^a \prod p_i^{k_i} \prod q_j^{r_j}$ where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ then

$$g(n) = \prod g(p_i^{k_i}) \prod g(q_j^{r_j}) = \prod (k_i + 1) \prod (0 \text{ or } 1)$$

and $g(n)$ is nonzero if and only if all exponents r_j are even in which case $g(n) = \prod (k_i + 1)$.

□

8. For a positive integer n let $\tau(n)$ be the number of positive divisors of n. Show that

$$D_{\tau^2}(s) = \frac{\zeta(s)^4}{\zeta(2s)}$$

Proof. As $\tau(n)$ is multiplicative

$$D_{\tau^2}(s) = \prod_p \left(\sum_{k\geq 0} \frac{\tau^2(p^k)}{p^{ks}} \right)$$

where $\tau(p^k) = k+1$.

We compute

$$\sum_{k\geq 0} \frac{(k+1)^2}{p^{ks}} = \frac{1+p^{-s}}{(1-p^{-s})^3}$$

as $\sum (k+2)(k+1)x^k = (\sum x^k)'' = 2(1-x)^{-3}$ and $\sum (k+1)x^k = (\sum x^k)' = (1-x)^{-2}$ which implies that $\sum (k+1)^2 x^k = \sum (k+2)(k+1)x^k - \sum (k+1)x^k = 2(1-x)^{-3} - (1-x)^{-2} = (1+x)(1-x)^{-3}$. Taking the product over p we see that $\prod (1-p^{-s})^{-1} = \zeta(s)$ and $\prod (1+p^{-s}) = D_\lambda(s)^{-1} = \zeta(s)/\zeta(2s)$ where λ is Liouville's function that I mentioned in class. Putting everything together we get that

$$D_{\tau^2}(s) = \frac{\zeta(s)^4}{\zeta(2s)}$$

□