

Math 567 Fall 2008 Number Theory I, Solutions 6

1. Show that $\left(\sum_{m|n} d(m)\right)^2 = \sum_{m|n} d(m)^3$. d and d^3 are multiplicative, hence so are the sums on either side. Moreover it is easily proved by induction on k that $\sum_{j=0}^k (j+1) = \frac{1}{2}(k+1)(k+2)$ and $\sum_{j=0}^k (j+1)^3 = \frac{1}{4}(k+1)^2(k+2)^2$.
2. Show that if $\sigma(n)$ is odd, then n is a square or twice a square. We have $\sigma(p^k) = 1 + p + \dots + p^k \equiv 1 + k \pmod{2}$ when $p > 2$ and $\equiv 1 \pmod{2}$ when $p = 2$. Hence, if $n = 2^a \prod_{p>2} p^{k_p}$ and $\sigma(n)$ is odd, then k_p is even for every $p > 2$, say $k_p = 2l_p$ and so if a is even, then n is a perfect square and if a is odd, then n is twice a perfect square.
3. Show that $\sum_{l|(m,n)} \mu(l)$ is 1 when $(m,n) = 1$ and is 0 otherwise. Hence prove that $\sum_{m=1; (m,n)=1}^n m = \frac{1}{2}n\phi(n)$ when $n > 1$. The first part follows from $\sum_{k|l} \mu(k) = 1$ or 0 according as $l = 1$ or not. Thus, when $n > 1$, $\sum_{m=1; (m,n)=1}^n m = \sum_{m=1}^n m \sum_{l|(m,n)} \mu(l) = \sum_{l|n} \mu(l) \sum_{m=1; l|m}^n m = \sum_{l|n} \mu(l) \frac{l}{2} \frac{n}{l} \left(\frac{n}{l} + 1\right) = \frac{n^2}{2} \sum_{l|n} \frac{\mu(l)}{l} + \frac{n}{2} \sum_{l|n} \mu(l) = \frac{1}{2}n\phi(n)$.
4. Let $\lambda(n) = (-1)^{\Omega(n)}$. Show that $\lambda(n) = \sum_{m^2|n} \mu(n/m^2)$. Obviously λ and the sum are multiplicative. When $n = p^k$ and $k = 2l$, $m = 1, p, \dots, p^l$ and the only non-zero term is 1 corresponding to $m = p^l$. When $n = p^k$ and $k = 2l - 1$, $m = 1, 2, \dots, p^{l-1}$ and the only non-zero term is -1 corresponding to $m = p^{l-1}$.
5. Define $f(n)$ to be $(-1)^{\frac{n-1}{2}}$ when n is odd, 0 when n is even. Show that f is totally multiplicative and is periodic with period 4. The periodicity is clear. Obviously $n_1 n_2$ is even iff at least one of n_1 and n_2 is even. In that case $f(n_1 n_2) = 0 = f(n_1) f(n_2)$. Suppose $n_1 n_2$ is odd. Then $n_1 n_2 - 1 = (n_1 - 1)(n_2 - 1) + n_1 + n_2 - 2 \equiv (n_1 - 1) + (n_2 - 1) \pmod{4}$.
6. Let $k \in \mathbb{N}$, $z \in \mathbb{C}$, $e(\alpha) = \exp(2\pi i \alpha)$. Define $\Phi_k(z) = \prod_{l=1; (l,k)=1}^k (z - e(l/k))$, the k -th cyclotomic polynomial, i.e. the monic polynomial whose roots are the primitive k -th roots of unity. (i) Show that $\prod_{l|k} \Phi_l(z) = z^k - 1$ and $\Phi_1(z) = z - 1$. (ii) Deduce that $\Phi_k(z) = \prod_{l|k} (z^l - 1)^{\mu(k/l)}$. (iii) Show that if $k > 1$, then $\Phi_k(z) = \prod_{l|k} (1 - z^l)^{\mu(k/l)}$ and $\Phi_k(0) = 1$. (iv) By considering the expansion $(1 - z^l)^{-1} = 1 + z^l + z^{2l} + \dots$ when $|z| < 1$ show that $\Phi_k(z)$ has integer coefficients. (v) Let K be the largest squarefree divisor of k . Show that $\Phi_k(z) = \Phi_K(z^{k/K})$. (vi) Prove that $\Phi_p(z) = 1 + z + \dots + z^{p-1}$. (vii) Show that if k is odd and $k > 1$, then $\Phi_{2^r k}(z) = \Phi_k(-z^{2^{r-1}})$. (viii) Suppose that p and q are different primes. Show that, when $|z| < 1$, $\Phi_{pq}(z) = (1 - z) \sum_{n=0}^{\infty} b_n z^n$ where b_n is the number of choices of $u, v \in \mathbb{Z}$ with $0 \leq u \leq q - 1$, $v \geq 0$ and $up + vq = n$. Deduce that $b_n = 0$ or 1 and that the coefficients of $\Phi_{pq}(z)$ are ± 1 or 0. (ix) Show that if $k < 105$, then the coefficients of $\Phi_k(z)$ are ± 1 or 0. (x) Show that the coefficient of z^7 in Φ_{105} is -2 . (xi) Prove that if $k > 1$, then $\Phi_k(1) = e^{\Lambda(k)}$. (i) $z^k - 1$ is the monic polynomial of degree k whose roots are the k -th roots of unity, $e(j/k)$, $1 \leq j \leq k$. Sort them according to $d = (j, k)$, take out the common factor d and observe that those with $k/d = l$ are precisely the roots of Φ_l . (ii) By (i), $\text{RHS} = \prod_{l|k} (\prod_{j|l} \Phi_j(z))^{\mu(k/l)} = \prod_{j|k} (\prod_{j|l|k} \Phi_j(z))^{\mu(k/l)} = \prod_{j|k} (\prod_{m|k/j} \Phi_j(z))^{\mu((k/j)/m)} = \prod_{j|k} \Phi_j(z)^{\sum_{m|k/j} \mu((k/j)/m)}$. (iii) If $k > 1$, then $(-1)^{\sum_{l|k} \mu(k/l)} = 1$. (iv) It is an immediate consequence of the Dirichlet product formula and induction that the product of the finite number of power series with integer coefficients if itself a power series with integer coefficients. (v) In (iii), $\mu(k/l)$ is non-zero iff $k/l = K/j$ with $j|K$, and then $l = (k/K)j$. (vi) By (iii), when $z \neq 1$, $\Phi_p(z) = (1 - z^p)/(1 - z)$. (vii) Each $l|2^r k$ is of the form $2^s m$ with $0 \leq s \leq r$, $m|k$. In (iii), when $s \leq r - 2$, $\mu(2^r k/l) = 0$. Thus $\Phi_{2^r k}(z) = \prod_{l|k} (1 - z^{2^{r-1}l})^{\mu(2k/l)} (1 - z^{2^r l})^{\mu(k/l)}$. Now the general term in the product is $(1 + z^{2^{r-1}l})^{\mu(k/l)}$ and $1 + z^{2^{r-1}l} = 1 - (-z^{2^{r-1}l})$. (viii). By (iii), when $|z| < 1$, $\Phi_{pq}(z) = (1 - z)(1 - z^p)^{-1} \frac{1 - z^{pq}}{1 - z^q} = (1 - z)(1 + z^p + z^{2p} + \dots)(1 + z^p + \dots + z^{p(q-1)})$ and rearranging the product of the last two factors gives $\sum_{n=0}^{\infty} b_n z^n$. In the definition of b_n we have $up \equiv n \pmod{q}$ and $0 \leq u \leq q - 1$. Thus u is uniquely determined. Moreover then there is at most one choice for v . Now the coefficient of z^n in Φ_{pq} is $b_n - b_{n-1}$. (ix) By (vii) we can assume that k is odd. Then by (v) we can suppose that k is squarefree. Since $k < 105$ we are then in cases (vi) or (viii). (x) By (iii), $\Phi_{105}(z) \equiv (1 - z)^{-1}(1 - z^3)(1 - z^5)(1 - z^7) \equiv (1 + z + \dots + z^7)(1 - z^3 - z^5 - z^7) \equiv 1 + z + z^2 - z^5 - z^6 - 2z^7 \pmod{z^8}$. (xi) When $k > 1$, since $\sum_{l|k} \mu(l) = 0$, when $z \neq 1$, by (ii), $\Phi_k(z) = \prod_{l|k} \left(\frac{z^l - 1}{z - 1}\right)^{\mu(k/l)}$. Now, by l'Hôpital's rule, $\Phi_k(1) = \lim_{z \rightarrow 1} \Phi_k(z) = \prod_{l|k} l^{\mu(k/l)} = \exp(\sum_{l|k} (\log l) \mu(k/l))$.