Math 571 Analytic Number Theory, Solutions 4

1. Given $k, q \in \mathbb{N}$, let $\rho(q;n)$ denote the number of solutions of $x^k \equiv n \pmod{q}$ and define $S(q,a) = \sum_{x=1}^{q} e(ax^k/q)$. (i) Prove that if $(n,q)=1$, then $\rho(q;n) = \sum_{x=1}^{q} \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \overline{\chi}(n)\chi(x)^k$ (ii) Deduce that, if $(n,q) = 1$, $\rho(q;n) = \sum_{\substack{\chi \pmod{q} \\ \chi^k=\chi_0}} \chi(n)$. (iii) Given a prime number p, let $\mathcal{A}$ denote the set of characters χ modulo p such that $\chi^k = \chi_0$ but $\chi \neq \chi_0$. Prove that if $p \nmid a$, then $S(p,a) = \sum_{\chi\in\mathcal{A}} \overline{\chi}(a)\tau(\chi)$. Let g be a primitive root modulo p. Prove that every character modulo p can be defined by $\chi_h(g^y) = e\left(\frac{hy}{p-1}\right)$. (v) Prove that $\operatorname{card}(\mathcal{A}) = (k,p-1)-1$ and deduce that $|S(p,a)| \le \big((k,p-1)-1\big)p^{\frac{1}{2}}$.

(i) By the orthogonality of the characters modulo q, the inner sum will be 0 unless $x^k \equiv n \pmod{q}$ and $(n,q)=1$, in which case it is $\phi(q)$. (ii) After interchanging the order in (i) we observe that $\sum_{x=1}^{q} \chi^k(x) = 0$ unless the character χ^k is the principal character, in which case it is $\phi(q)$. (iii) By definition of S and ρ, $S(p,1) = 1 + \sum_{n=1}^{p-1} e(an/p)\rho(p;n)$. By (ii) this is $1 + \sum_{\substack{\chi \pmod{q} \\ \chi^k=\chi_0}} \sum_{n=1}^{p} e(an/p)\chi(n) = \sum_{n=1}^{p} e(an/p) + \sum_{\chi\in\mathcal{A}} \sum_{n=1}^{p} e(an/p)\chi(n)$, and the first sum sums to 0. When $\chi \neq \chi_0$, since p is prime χ will be primitive so then sum over n is $\overline{\chi}(a)\tau(\chi)$. (iv) The given construction gives $\phi(p)$ multiplicative functions of period p so must give an isomorphism. By (iv), for χ^k to be equal to χ_0 we must has $p-1|hk$, i.e. $\frac{p-1}{(p-1,k)}|h$ and so there are only $(p-1.k)$ possibilities, and one will be the principal character.

2. Here is a proof of a slightly weaker result avoiding characters. (i) With the same notation, prove that if $1 \le y \le p-1$, then $S(p,a) = S(p,ay^k)$. (ii) Prove that if $p \nmid n$, then there is an m with $1 \le m \le p-1$ such that $\rho(p;n) = \operatorname{card}\{y : 1 \le y \le p-1, g^{yk} \equiv g^m\}$ and that $\rho(p;n) \le (k,p-1)$. (iii) Prove that if $p \nmid a$, then $(p-1)|S(p,a)|^2 = \sum_{z=1}^{p-1} \rho(p;z)|S(p,az)|^2 \le (k,p-1)\sum_{t=1}^{p-1} |S(p,t)|^2$. (iv) Prove that $\sum_{t=1}^{p} |S(p,t)|^2 = \sum_{x=1}^{p} p\rho(p;x^k) \le p(p-1)(k,p-1)+p$, (v) Deduce that $|S(p,a)| \le \big((k,p-1)((k,p-1)-1)\big)^{1/2} p^{1/2}$.

(i) Simply observe that xy runs through a complete set of residue as x does. (ii) Immediate by substitution $x = g^y$, $n = g^m$. Then ρ is the number of solutions of $yk \equiv m \pmod{p-1}$. (iii) Sum over $y \not\equiv 0$ and sort according as $y^k \equiv z$. (iv) By orthogonality of the additive characters we are counting solutions of $x^k \equiv y^k$ with weight p and for a given x the number of such is $\rho(p; x^k)$ and this is 1 when $x = p$ and $\le (k, p-1)$ otherwise. (v) By (iii) and (iv) $(p-1)|S(p,a)|^2 \le (k,p-1)\big(p(p-1)(k,p-1) - p(p-1)\big)$. It ought to be possible to tighten this up to give 1(v).

3. (Mordell c1930) (i) Let $N_k(p)$ denote the number of solutions in $x_1, \dots, x_k, y_1, \dots, y_k$ of the simultaneous congruences

$$\begin{aligned} x_1 + \cdots x_k &\equiv y_1 + \cdots y_k \pmod p \\ x_2 + \cdots x_2 &\equiv y_2 + \cdots y_k^2 \pmod p \\ &\vdots \\ x_1^k + \cdots x_k^k &\equiv y_1^k + \cdots y_k^k \pmod p \end{aligned}$$

Prove that if $k < p$, then $N_k(p) \le k! p^k$.

In fact it can be shown that the $\mathbf{y}$ are a permutation of the $\mathbf{x}$. Let $\sigma_j(\mathbf{x})$ denote the elementary symmetric polynomial of degree j in $x_1, \dots, x_k$ and let $s_j(\mathbf{x}) = \sum_{r=1}^k x_r^j$. Then Newton's identities state that $j\sigma_j(\mathbf{x}) = \sum_{r=1}^j (-1)^{r-1} \sigma_{j-r}(\mathbf{x}) s_r(\mathbf{x})$ valid for $k \ge j \ge 1$ and $0 = \sum_{r=j-k}^j (-1)^{r-1} \sigma_{j-r}(\mathbf{x}) s_r(\mathbf{x})$ valid for $j > k \ge 1$. The system of congruences tells that $s_r(\mathbf{x}) \equiv s_r(\mathbf{y}) \pmod p$ for $1 \le r \le k$ and hence likewise the $\sigma_r(\mathbf{x})$ and $\sigma_r(\mathbf{y})$. Thus for the polynomial $P(x; \mathbf{u}) = (x - u_1) \dots (x - u_k)$, for any solution of the system one has $P(x; \mathbf{x}) \equiv P(x; \mathbf{y}) \pmod p$. It then follows that $y_k \equiv x_j$ for some j and then by induction that the $\mathbf{y}$ are a permutation of the $\mathbf{x}$ modulo p. (ii) Let $f(x) = a_1 x + \cdots + a_k x^k$ and $S(p; f) = S(p; \mathbf{a}) = \sum_{x=1}^p e\big(f(x)/p\big)$. Show that $\sum_{a_1}^p \dots \sum_{a_k}^p |S(p; \mathbf{a})|^{2k} = p^k N_k(p)$ (iii) Show that if $p \nmid y$ and $z \in \mathbb{Z}$, then $S(p; \mathbf{a}) = S(p; \mathbf{b})$ where $b_k = a_k y^k$ and $b_{k-1} = (k a_k z + a_{k-1}) y^{k-1}$ and hence that $p \frac{p-1}{(k,p-1)} |S(p; \mathbf{a})|^{2k} \le k! p^{2k}$. (iv) Prove Mordel's theorem that if f is a polynomial with integer coefficients of degree k modulo p, then $|S(p; f)| \le k p^{1-1/k}$.

(ii) This follows by writing each term as a $2k$-iterated sum and applying orthogonality. (iii) Replace the summation variable x in $S(p; f)$ by $xy + z$. Then the leading term becomes $a_k y^k$ and the coefficient of x^{k-1} is $a_k y^{k-1} z + a_{k-1} y^{k-1}$, and this gives $(p-1)/(k, p-1)$ different possible b_k modulo p and for each such y there are p different possible choices for z, and hence for b_k. Thus we cover at least $p(p-1)/(k, p-1)$ different choices for $\mathbf{a}$. (iv) It follows that $S(f; p)| \le (2k.k!)^{\frac{1}{2k}} p^{1/2} \le k p^{1-1/k}$. One only needs to check that for $k \ge 3$ one has $k^{-1} (2k.k!)^{\frac{1}{2k}} \le 1$.