UNIVERSITY OF NEW SOUTH WALES.
SCHOOL OF MATHEMATICS AND STATISTICS
MATH5645
TOPICS IN ANALYTIC NUMBER THEORY

6. GAUSS SUMS:

1 If $g_a = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$ and $g = g_1$, prove (directly) that

a. $g_a = \left(\frac{a}{p}\right) g$

b. $g^2 = (-1)^{\frac{p-1}{2}} p$.

2 If $g_a = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$, find $\sum_{a=1}^{p-1} g_a$.

***3** By evaluating $\sum_t (1 + \left(\frac{t}{p}\right))\zeta^t$ in two ways prove that $g = \sum_t \zeta^{t^2}$.

4 Verify the result $g^2(\chi) = (-1)^{\frac{p-1}{2}} p$, (for χ not principal) in the case $p = 3$.

5 For p prime, if $(n, p-1) = d$ then $x^n \equiv a \bmod p$ has exactly d solutions in $\mathbf{Z}_p$ iff $a^{\frac{p-1}{d}} \equiv 1 \bmod p$.

***6** **a.** Prove that the group of characters in $\mathbf{Z}_p$ is a cyclic group of order $p - 1$.

b. If $a \in \mathbf{Z}_p$ and $a \neq 1$, then there exists a character χ such that $\chi(a) \neq 1$.

(Hint for (b): If g is a primitive root mod p, define $\lambda(g^k)$ by $e^{2\pi ik/(p-1)}$.)

7 If $a \in \mathbf{Z}_p$ and $n|p-1$ and $x^n \equiv a \bmod p$ is not soluble, prove that there exists a character χ such that $\chi^n = \chi_1$ and $\chi(a) \neq 1$.
(Hint: Put $\chi = \lambda^{\frac{p-1}{n}}$, with λ as in previous question.)

8 Prove that $\overline{g(\chi)} = \chi(-1) g(\overline{\chi})$.

9 Prove that if $p \equiv 1 \bmod n$, and χ is a character of order n, then

$$(g(\chi))^n = \chi(-1) p J(\chi, \chi) J(\chi, \chi^2) \dots J(\chi, \chi^{n-2}).$$

10 Find the number of solutions to $x^n + y^n \equiv 1 \bmod 19$ for $n = 2$ and $n = 3$.

***11** Let χ be a non-trivial character modulo p and ρ be the quadratic character mod p, (i.e. ρ is the Legendre symbol.)

a. Use the fact that $N(x^2 = a) = 1 + \rho(a)$ to show that $J(\chi, \rho) = \sum_t \chi(1 - t^2)$.

b. If $p \not| k$, show that $\sum_t \chi(t(k-t)) = \chi\left(\frac{k^2}{2^2}\right) J(\chi, \rho)$.

(Hint: Put $u = \frac{k}{2}(t+1)$.)

***12** Suppose $p \equiv 1 \bmod 4$, ψ is a character of order 2 (i.e. the Legendre symbol) and χ is a character of order 4. Also let $z = -J(\chi, \psi)$.

a. Prove that z is a Gaussian integer $a + ib$ and

$$J(\psi, \chi) + J(\psi, \chi^3) = -2a,$$

with $p = a^2 + b^2$.

b. Prove that if $a + ib \equiv 1 \bmod 2 + 2i$ then a is odd and b is even. Further show that $4|b \Rightarrow a \equiv 1 \bmod 4$ and $4 \not| b \Rightarrow a \equiv -1 \bmod 4$.

c. Show that $N(x^2 + y^4 \equiv 1 \bmod p) = p - 1 - 2a$, where $a + ib \equiv 1 \bmod 2 + 2i$ and $p = a^2 + b^2$.

d. Using the transformation $(x, y) \rightarrow ((1 + x^2)y, x)$ show that $N(x^2 + y^2 + x^2y^2 \equiv 1) = p - 3 - 2a$.

e. Illustrate the result in (b) for $p = 5$.

(The result in (c) was conjectured by Gauss and appears as the last entry in his mathematical diary.)

1 **a.** $g_a\left(\frac{a}{p}\right) = \sum_{t=1}^{p-1}\left(\frac{at}{p}\right)\zeta^{at} = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\zeta^t = g$. **b.** Let $T = \sum_{a=0}^{p-1} g_a g_{-a}$, $a \not\equiv 0 \bmod p$. Now $g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)g^2 = \left(\frac{-1}{p}\right)g^2$, so $T = \left(\frac{-1}{p}\right)g^2(p-1)$. Also $g_a g_{-a} = \sum_x\sum_y\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}$, hence $\sum_a g_a g_{-a} = \sum_x\sum_y\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\sum_a\zeta^{a(x-y)} = \sum_x\sum_y\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)p$. The sum of the terms from $x \neq y$ is zero, so this sum is $p(p-1)$, i.e. $g_a g_{-a} = p(p-1)$. Equating the two values of T the result follows.

2 Use $g_a = \left(\frac{a}{p}\right)g$ and the sum has the value 0.

3 $\sum_t(1+\left(\frac{t}{p}\right)\zeta^t = \left(\frac{t}{p}\right)\zeta^t = g$. Also, since $x^2 \equiv a \bmod p$ has solutions iff $\left(\frac{t}{p}\right) = 1$ and the number of solutions of this equation is $(1+\left(\frac{a}{p}\right))$, $\sum_t\zeta^{t^2} = \sum_a(1+\left(\frac{a}{p}\right))\zeta^a = \sum_t(1+\left(\frac{t}{p}\right))\zeta^t$. Hence $g = \sum_t\zeta^{t^2}$.

4 For $p = 3$, $\zeta^3 = 1$ and there is only one non-principal character, χ with $\chi(0) = 0, \chi(1) = 1, \chi(2) = -1$, hence $g^2(\chi) = \left(\sum_{t=0}^{2}\chi(t)\zeta^t\right)^2 = (\zeta-\zeta^2)^2 = -3$.

5 Let g be a primitive root mod p, then $x^n \equiv a \bmod p \Leftrightarrow n\, ind_g x \equiv ind_g a \bmod p-1$, we have $(n,p-1) = d$ solutions iff $d|ind_g a$. Let $b = ind_g a$ then $a = g^b$. If $d|b$ then $1 \equiv g^{\frac{b(p-1)}{d}} \bmod p = a^{\frac{p-1}{d}}$ and conversely if $a^{\frac{p-1}{d}} \equiv 1 \bmod p$ then $g^{\frac{b(p-1)}{d}} \equiv 1$ and this implies $d|b$.

6 **a.** $\mathbf{Z}_p$ is cyclic, so let g be a generator (p.r.). Hence $a \in \mathbf{Z}_p \Rightarrow a = g^t$ for some t and $\chi(a) = \chi(g^t) = (\chi(g))^t$. So $\chi(a)$ is completely determined by $\chi(g)$ which is a $p-1$st root of unity ($\neq 1$).The group of characters is thus generated by $\chi(g)$ which has order $p-1$. **b.** Set $\lambda(g^k) = e^{2\pi ik/(p-1)}$, then λ is a well-defined character. If $\lambda^n = \lambda_1$ then $\lambda^n(g) = \lambda_1(g) = 1$. But $\lambda^n(g) = (\lambda(g))^n = e^{\frac{2\pi in}{p-1}} \Rightarrow p-1|n$. Also $\lambda^{p-1}(a) = (\lambda(a))^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$ so $\lambda^{p-1} = \lambda_1$. Hence $\lambda_1, \lambda, \lambda^2, \ldots\lambda^{p-2}$ are distinct so λ is a generator of the group of characters. If $a \neq 1$, is an element of $\mathbf{Z}_p$ then $a = g^\ell$ and $p-1 \not|\ell$. Thus $\lambda(a) = \lambda(g^\ell) = e^{\frac{2\pi i\ell}{p-1}} \neq 1$.

7 Let $\chi = \lambda^{\frac{p-1}{n}}$, with λ as in previous question, and g a primitive root mod p. Then $\chi(g) = \lambda^{\frac{p-1}{n}}(g) = \lambda(g^{\frac{p-1}{n}}) = e^{\frac{2\pi i}{n}}$. Now $a = g^\ell$ for some ℓ and so $x \equiv a$ not soluble implies $n \not|\ell$. Hence $\chi(a) = \chi(g)^\ell = e^{\frac{2\pi i\ell}{n}} \neq 1$. Finally, $\chi^n = \lambda^{p-1} = \chi_1$.

8 $\overline{g(\chi)} = \sum_t\overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_t\overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi})$.

9 Using $g(\chi)g(\lambda) = g(\chi\lambda)J(\chi,\lambda)$, we have $(g(\chi))^2 = J(\chi,\chi)g(\chi^2) \Rightarrow (g(\chi))^3 = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$. Continuing thus, $g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)J(\chi,\chi^3)\ldots J(\chi,\chi^{n-2})g(\chi^{n-1})$ $(*)$. Now $g(\chi^{n-1}) = g(\chi^{-1}) = g(\overline{\chi})$ and $g(\chi)g(\overline{\chi}) = \chi(-1)p$. Multiply (*) by $g(\chi)$ and the result follows.

10 20 and 24.

11 **a.** $J(\chi,\rho) = \sum_u\chi(1-u)\rho(u) = \sum_t\chi(1-u)(1+\rho(u))$. Now $1+\rho(u) = 0$ is u is not a square, so $J(\chi,\rho) = \sum_t\chi(1-t^2)$. **b.** Put $u = \frac{k}{2}(t+1)$, then $\chi(\frac{k^2}{2^2})J(\chi,\rho) = \sum_t\chi(\frac{k^2}{2^2})\chi(1-t^2) = \sum_u\chi\left((\frac{k^2}{2^2})(\frac{2u}{k})(2-\frac{2u}{k})\right) = \sum_u\chi(u(k-u)$ and the result follows.

12 **a.** χ takes values from $\{1,-1,i,-i\}$ and ψ from $\{1,-1\}$ hence the Jacobi symbol is a gaussian integer, $z=a+ib$. Also $|J(\chi,\psi)|=\sqrt{p}$. Finally $\chi^3=\overline{\chi}$ so $J(\psi,\chi)+J(\psi,\chi^3)=J(\psi,\chi)+\overline{J(\psi,\chi)}=-z-\overline{z}=-2a$. **b.** $a+ib\equiv 1 \bmod (2+2i) \Rightarrow a$ odd and b even. Also $2+2i|4$ so $4|b \Rightarrow a+ib\equiv a\equiv 1 \bmod 2+2i$. Taking conjugates and multiplying $(a-1)^2\equiv 1 \bmod 8 \Rightarrow a\equiv 1 \bmod 4$. If $4 \not| b$ then $b=4k+2$ so $a+ib\equiv 2+2i$ mod $(2+2i)$. Now $2i\equiv -2(2+2i) \Rightarrow a\equiv 3\equiv -1 \bmod 2+2i$ and as before $8|(a+1)^2 \Rightarrow a\equiv -1$ mod 4. **c.** $N(x^2+y^4\equiv 1 \bmod p)=\sum\limits_{a+b=1} N(x^2=a)N(x^4=b)=\sum\limits_{a+b=1}(1+\psi(a))(1+\chi(b)+\chi^2(b)+\chi^3(b))=$ $p+J(\psi,\chi)+J(\psi,\chi^2)+J(\psi,\chi^3)=p-2a+J(\psi,\chi^2)$. Now $\chi^2=\psi=\overline{\psi}$ so $J(\psi,\chi^2)=-\psi(-1)=-1$ (since $p\equiv 1 \bmod 4$.). The result follows. We also have to prove that $a+ib\equiv 1 \bmod (2+2i)$. Note that for $a,b\neq 0$ we have $\psi(a)-1\equiv 0 \bmod 2$ and $\chi(a)-1\equiv 0 \bmod 1+i$, since $2=-i(1+i)^2$ and $-1+i=i(1+i)$. Thus if $a,b\neq 0$, we have $(\psi(a)-1)(\chi(b)-1)\equiv 0 \bmod (2+2i)$, and this is still true for the cases $(a,b)=(1,0),(0,1)$ (trivially). Hence $\sum\limits_{a+b=1}(\psi(a)-1)(\chi(b)-1)\equiv 0 \bmod 2+2i$. Expanding we have $z\equiv p \bmod 2+2i$. Now $p\equiv 1$ mod 4 and $4|2+2i$ so $p\equiv 1 \bmod 2+2i$ and so $z\equiv 1 \bmod 2+2i$. **d.** The given map is 1-1 but not onto as the inverse is not defined for $\{0,\pm y\}$ when $y^2\equiv -1 \bmod p$. Hence there are 2 fewer points. **e.** $5=1^2+2^2$, and $4 \not| 2$ so take $a=-1$. The solutions to $x^2+y^4=1 \bmod 5$ are $(0,y),(y=1,2,3,4);(1,0),(4,0)$. Thus $N=6=5-1+2$.

P. Brown/5645/2008/problem˙sheet˙6.tex