SOME CONGRUENCES IN ALGEBRAIC INTEGERS AND RATIONAL INTEGERS

by A. R. RAJWADE, *Department of Mathematics, Panjab University, Chandigarh*

(Communicated by F. C. Auluck, F. N. A.).

(Received 15 December 1973 ; after revision 27 March 1974)

Using Gauss' cyclotomic numbers a congruence relating to the factor in $Z[\omega]$ of a rational prime $p \equiv 1 \pmod 3$ is derived, and a classical congruence due to Jacobi proved as a corollary.
For primes $p \equiv 1 \pmod 5$ the following congruence is proved : Let $p = 1+5n$ and let x be uniquely determined by Dickson's theorem (1935, p, 402 Theorem 8). Then

$$x + \binom{4n}{n} + \binom{3n}{n} \equiv 0 \pmod p.$$

For the convenience of the reader, we define Gauss' cyclotomic numbers. Let $p=ef+1$ be a prime and let g be a primitive root mod p. For integers h, k we define the cyclotomic constants (h, k) to be the number of pairs of integers u, v satisfying

$$1+g^{eu+h} = g^{ev+k} \pmod p \quad (0 \leqslant u, v \leqslant f-1).$$

Clearly (h, k) depends only on the residue classes of h and k mod e. It is easy to verify the following identities :

$$(h, k) = (-h, k-h).$$

$$(h, k) = (k, h) \text{ if } f \text{ is even.}$$

$$(h, k) = (k+e/2, h+e/2) \text{ if } f \text{ is odd.}$$

$$\sum_{k=0}^{e-1} (h, k) = f-n_h \quad (0 \leqslant h \leqslant e-1), \text{ where}$$

$n_h = 1$ if $h=0$ and f is even, or if $h=e/2$ and f is odd and $n_h = 0$ in all the other cases. (see, for example, Dickson 1935, 394).

§ 1. $p \equiv 1$ (*mod* 3)

Write $p = 1+3n$ (p prime) and factorize p in the Eisenstein integers $Z[\omega]$, where $\omega = (-1+\sqrt{-3})/2$, as $p = \pi\bar{\pi}$. This is uniquely possible with

the condition $\pi,\ \bar{\pi} \equiv -1 \pmod 3$. Write $\pi = a+b\omega$, $\bar{\pi} = a + b\omega^2$ so that $a \equiv -1 \pmod 3$, $b \equiv 0 \pmod 3$. Let g be a primitive root mod p and let, without loss of generality, $(g/\pi)_3 = \omega = \chi(g)$ where χ is the cubic character defined by $\chi(g^\nu) = \omega^\nu$, $\chi(0) = 0$. Consider the sum

$$\mathcal{V} = \sum_{v \pmod p} \chi(v) \cdot \chi(v+1).$$

$\mathcal{V}$ is the special Jacobi function $R(1, 1)$ in the notation of Dickson (1935) for which the relation $\mathcal{V}\,\bar{\mathcal{V}} = p$ is well known. In terms of the Gauss' cyclotomic numbers (i, j) $(0 \leqslant i, j \leqslant 2)$ for the factorization $p-1 = 3n$,

$$\begin{aligned}\mathcal{V} &= [(0, 0)+2(1, 2)-3(1, 1)]+3\omega[(2, 2)-(1, 1)] \\ &\qquad \text{(see Dickson 1935 or Rajwade 1969, p. 64)} \\ &= (A+2D-3B)+3\omega(C-B) \text{ in the notation of Rajwade (1969)} \\ &\equiv -1 \pmod 3 \quad (\text{since } A+1=D).\end{aligned}$$

Note also that $\mathcal{V}\,\bar{\mathcal{V}} = p$ follows directly form these considerations as has been done by Rajwade (1969). It follows that $\mathcal{V}$, $\bar{\mathcal{V}}$ are π, $\bar{\pi}$ in some order. Because of the condition $(g/\pi)_3 = \omega$ it can be shown that $\mathcal{V} = \pi$, $\bar{\mathcal{V}} = \bar{\pi}$. In fact

$$\begin{aligned}\mathcal{V} &= \sum \chi(v) \cdot \chi(v+1) \\ &= \sum (v/\pi)_3 \cdot ((v+1)/\pi)_3 \\ &\equiv \sum v^{p(-1)/3} \cdot (v+1)^{(p-1)/3} \pmod \pi \\ &\equiv \sum v^n \cdot (1+nv+\ldots+v^n) \pmod \pi.\end{aligned}$$

Here the exponent j of each power of v is $\leqslant 2n < p-1$ and so $p-1$ does not divide j. It follows that $\sum v^j \equiv 0 \pmod p$ and so $\equiv 0 \pmod \pi$. Thus the entire sum $\equiv 0 \pmod \pi$, i.e. $\pi \mid \mathcal{V}$ and so $\mathcal{V} = \pi$. We are now ready to prove a few results.

Proposition 1— $\pi \equiv -\binom{2n}{n} \pmod{\bar{\pi}}$.

Proof:
$$\begin{aligned}\mathcal{V} = \pi &= \sum \chi(v) \cdot \chi(v+1) = \sum (v/\pi)_3 \cdot ((v+1)/\pi)_3 \\ &= \sum (v/\bar{\pi})_3^2 \cdot ((v+1)/\bar{\pi})_3^2 \\ &\equiv \sum v^{2n} \cdot (1+v)^{2n} \pmod{\bar{\pi}} \\ &= \sum v^{2n}(1+2nv+\ldots+v^{2n}) \pmod{\bar{\pi}}.\end{aligned}$$

Here, as above, each term is divisible by p except one where the exponent of v is divisible by $p-1$, viz. $\sum v^{2n}\binom{2n}{n} \cdot v^n$, and this is $\equiv -\binom{2n}{n} \pmod{\bar{\pi}}$ as desired.

Rewriting proposition 1 we get

$$\pi + \binom{2n}{n} = \lambda\bar{\pi}, \qquad \lambda \in Z[\omega]$$

and by symmetry $\quad \bar{\pi} + \binom{2n}{n} = \mu\pi, \qquad \mu \in Z[\omega]$

Multiplying $\quad p + \binom{2n}{n}(\pi+\bar{\pi}) + \binom{2n}{n}^2 = \lambda\mu p.$

Here the left-hand side $\in Z$ hence so does the right-hand side, i.e. p divides $\binom{2n}{n}\left[\binom{2n}{n} + (\pi+\bar{\pi})\right]$ in Z. Since p does not divide $\binom{2n}{n}$ and $\pi+\bar{\pi} = 2a-b$ we get

Proposition 2—Let $p=3n+1$ be prime and write $p = a^2-ab+b^2 \quad (=\pi\bar{\pi})$ with $a \equiv -1 \pmod 3$, $b \equiv 0 \pmod 3$ uniquely. Then

$$\binom{2n}{n} \equiv b-2a \pmod p.$$

(This formula is due to Jacobi 1872).

§ 2. $p \equiv 1 \pmod 5$

The set up is as in § 1. Write $p = 5n+1$ and let $\zeta = e^{2\pi i/5}$. p factorizes in $Z[\zeta]$ into four factors $p = \pi_1\pi_2\pi_3\pi_4 = \pi_1\pi_2\bar{\pi}_2\bar{\pi}_1$, where we number these to satisfy $(g/\pi_i)_5 = \zeta^i$, where g is a primitive root mod p. A quintic character χ is defined by $\chi(g^\nu) = \zeta^\nu$, $\chi(0) = 0$, so that $(g/\pi_i)_5 = \chi^i(g)$.

Let $\qquad T = \Sigma\,\chi(v).\,\chi(v+1), \quad S = \Sigma\,\chi^2(v).\,\chi^2(v+1).$

These are the special Jacobi functions again, viz. $R(1,1)$ and $R(2,2)$ for which the relations $T\bar{T} = p = S\bar{S}$ are well known (Dickson 1935, see also Rajwade 1969, p. 68). It follows that $T, \bar{T}, S, \bar{S}$ are just $\pi_1\pi_2$, $\pi_1\pi_3$, $\pi_2\pi_4$, $\pi_3\pi_4$ in some order. Because of the conditions $(g/\pi_i)_5 = \zeta^i$ we can show that $T = \pi_1\pi_3$, $S = \pi_1\pi_2$ (see page 69 of Rajwade 1969 in this very notation).

But now the units of $Z[\zeta]$ are $\pm\zeta^i((1+\sqrt{5})/2)^j$, $0 \leqslant i \leqslant 4$, $j \in Z$ and so the π_j can not be fixed by any finite number of congruences. However, we claim that the T (and similarly $\bar{T}$, S, $\bar{S}$) are uniquely fixed by the following two conditions :

$$T(\zeta) \equiv T(1) \pmod{(1-\zeta)^3} \tag{1}$$

$$T(1) \equiv -1 \pmod 5. \tag{2}$$

This can be done by the use of Gauss' cyclotomic constants for the factorization $p-1 = 5n$ — in fact more than (1) is true, viz.

$$T(\zeta) \equiv T(1) \pmod{(1-\zeta)^3}. \tag{2a}$$

For a proof see Rajwade (1973).

Note that to get the T (and $\bar{T}$, S, $\bar{S}$) we factorize $p = \pi_1 \pi_2 \pi_3 \pi_4$ anyhow with $(g/\pi_i)_5 = \zeta^i$ and then $\pi_1 \pi_3$ (and $\pi_4 \pi_2$, $\pi_1 \pi_2$, $\pi_4 \pi_3$) can be made to satisfy (1) and (2) on multiplication by a root of unity (Rajwade 1973). Thus getting T, $\bar{T}$, S S is an easy job from the factorization $p = \pi_1 \pi_2 \pi_3 \pi_4$; one does not have to evaluate $\sum \chi(v).\chi(v+1)$ term by term.

In terms of the cyclotomic constants the T and S are

$$\begin{aligned} R(1,1) = T = {} & \zeta(2E+D-2Y-A)+\zeta^2(2D+B-2Z-A) \\ & +\zeta^3(2C+E-2Z-A)+\zeta^4(2B+C-2Y-A) \end{aligned} \tag{3}$$

$$\begin{aligned} R(2,2) = S = {} & \zeta(2C+E-2Z-A)+\zeta^2(2E+D-2Y-A) \\ & +\zeta^3(2B+C-2Y-A)+\zeta^4(2D+B-2Z-A) \end{aligned} \tag{4}$$

and these constants A, B, C, D, E, Y, Z satisfy the well known relations

$$\left.\begin{aligned} A+B+C+D+E &= n-1 \\ 2Y+Z+B+E &= n \\ Y+2Z+C+D &= n \end{aligned}\right\}. \tag{5}$$

(For all this see Dickson 1935 or in this very notation Rajwade 1969).

We now have the following.

Proposition 3

$$(i) \quad T \equiv -\binom{3n}{n} \pmod{\pi_2}$$

$$(ii) \quad T \equiv -\binom{4n}{n} \pmod{\pi_4}$$

$$(iii) \quad S \equiv -\binom{4n}{n} \pmod{\pi_3}$$

$$(iv) \quad S \equiv -\binom{3n}{n} \pmod{\pi_4}.$$

Proof : We have $T = \sum (\chi^2(v))^3 (\chi^3(v+1))^2$

$$\equiv \sum v^{3n}(1+v)^{3n} \pmod{\pi_2}$$

$$\equiv \sum v^{3n}(1+3nv+\ldots+v^{3n} \pmod{\pi_2}.$$

Here all the terms are divisible by p (and so by π_2) since

$\Sigma v^j \equiv 0 \pmod{p}$ if $p-1$ does not divide j, except when $r = 2n$ when $\Sigma v^j \equiv -1 \pmod{p}$. Hence $T \equiv -\binom{3n}{2n} \pmod{\pi_2}$

$$\equiv -\binom{3n}{n} \pmod{\pi_2} \text{ as required.}$$

To get (*ii*) write $T = \Sigma (\chi^4 (v))^4 . (\chi^4 (v+1))^4$ and proceed as above. As for (*iii*) and (*iv*) write $S = \Sigma (\chi^3 (v))^4 (\chi^3 (v+1))^4$ and $S = \Sigma (\chi^4 (v))^3 . (\chi^4 (v+1))^3$ respectively and proceed as usual.

This completes the proof of the proposition.

Now $\bar{T} = \pi_2 \pi_4 \equiv 0 \pmod{\pi_4}$ and $\bar{S} = \pi_3 \pi_4 \equiv 0 \pmod{\pi_4}$. Adding these and (*ii*) and (*iv*) of Proposition 3 gives :

$$T+\bar{T}+S+\bar{S} \equiv -\binom{4n}{n} - \binom{3n}{n} \pmod{\pi_4}. \tag{6}$$

But in terms of the cyclotomic constants, we have

$$S+\bar{S} = -(p+1) + \frac{25}{2}(Y+Z) + \frac{5\sqrt{5}}{2}(Y-Z)$$

$$T \cdot \bar{T} = -(p+1) + \frac{25}{2}(Y+Z) - \frac{5\sqrt{5}}{2}(Y-Z).$$

This follows by (3) and ($\bar{3}$) (and (4) and ($\bar{4}$)) and using (5) to eliminate $B+E$, $C+D$ and A from it. Note also that $\zeta = e^{2\pi i/5}$, hence $\zeta+\zeta^{-1} = 2\cos(2\pi/5) = (\sqrt{5}-1)/2$ and $\zeta^2+\zeta^{-2} = -\left(\frac{\sqrt{5}+1}{2}\right)$. Hence $S+\bar{S}+T+\bar{T} = -2(p+1)+25(Y+Z) = x$ where, by the famous theorem of Dickson's 1935, theorem 8, p. 102) we have

$$\begin{cases} 16p = x^2+50u^2+50v^2+125w^2 \\ v^2 \quad 4uv-u^2 = xw \\ x \equiv 1 \pmod{5} \ (x \text{ is unique with this condition}). \end{cases} \tag{7}$$

Hence (6) gives the following.

Proposition 4—Let $p=5n+1$ be prime and let x be uniquely determined by (7). Then

$$\binom{4n}{n} + \binom{3n}{3} + x \equiv 0 \pmod{p}.$$

REFERENCES

Dickson, L. E. (1935). Cyclotomy, higher congruences and Warings problem. ***Am. J. Math.***, **57** 391-424.

Jacobi. K. (1872), De residuis cubicis commetatic numersoa. ***J. angew. Math.***, **2** 66-69.

Rajwade, A. R. (1969), On rational primes p congruent to 1 (mod 3 or 5). ***Proc. Camb. Phil. Soc.***, **66**, 61-70.

—— (1973). On the congruence $y^2 = x^6 - a \pmod{p}$. ***Proc. Camb. phil. Soc.***. 74 473-75