Werk

Titel: Mathematische Annalen
Ort: Leipzig
Jahr: 1907
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0063
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0063

LOG Id: LOG_0009
LOG Titel: Sulla risoluzione apiristica delle congruenze binomie secondo un modulo primo
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN235181684
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Sulla risoluzione apiristica delle congruenze binomie secondo un modulo primo.

Di

MICHELE CIPOLLA a Palermo.

1. Il problema che ci proponiamo di risolvere nella presente nota, è il seguente: *Data una congruenza binomia*

$$x^n \equiv a \pmod{p}, \tag{1}$$

essendo p un numero primo dispari ed a un numero intero arbitrario non divisibile per p, determinare un polinomio in a, che fornisca una soluzione della congruenza (1) *per ogni residuo n-ico del modulo p.*

La questione risoluta da recente per il caso in cui n sia una potenza di 2*) non è stata finora trattata in generale.

Si può supporre, senza ledere la generalità, che il grado n della congruenza (1) sia un divisore di $p-1$, nel quale caso perchè la (1) sia possibile occorre e basta che sia

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p}. \tag{2}$$

Diremo che un polinomio della forma

$$A_0 + A_1 a + A_2 a^2 + \cdots + A_{\frac{p-1}{n}-1} a^{\frac{p-1}{n}-1} \tag{3}$$

è una *soluzione apiristica* della (1), quando, per ogni numero a soddisfacente alla condizione (2), esso è una soluzione della congruenza (1).

*) Tonelli, Rend. della R. Acc. dei Lincei, a. 1892, 1° sem., p. 116; a. 1893, 1° sem., p. 259. Si veggano anche le nostre note nel Rend. della R. Acc. di Napoli, a. 1903, fasc. 5°; a. 1904, fasc. 3° e 4°; a. 1905, fasc. 1° e fasc. 5°. — Per il caso di $n = 2$ una formola non diversa da quella da noi comunicata alla R. Accademia di Napoli (Rendiconti, fasc. 1°, gennaio 1905; v. formola (8) della presente nota) hanno dato in questi »Annalen« (v. 62, p. 409—412) i Sigg. Tamarkine e Friedmann. Anche per questo caso noi qui daremo formole molto più vantaggiose. — Per la letteratura sulla teoria delle congruenze si vegga la nostra monografia: *Theoria de congruentias intra numeros integro,* Revue de Math., publiée par G. Peano, Torino 1905.

La determinazione dei coefficienti A_i di una soluzione apiristica è fondata sul seguente concetto.

2. In un sistema completo di resti secondo il modolo p, possono scegliersi $\frac{p-1}{n}$ numeri, e non più, le cui potenze n^{ime} siano tutte incongrue fra loro (mod. p): un tal sistema lo diremo *un sistema completo di n^{imo} grado (mod. p)*.

Per determinare un sistema completo di n^{imo} grado distribuiamo in quadro i numeri di un sistema completo di resti (mod. p), (i quali formano un gruppo secondo il modolo p) rispetto ai numeri

$$(A) \qquad 1, \gamma_1, \gamma_2, \cdots, \gamma_{n-1},$$

formanti un sistema completo (gruppo) di soluzioni della congruenza

$$(4) \qquad x^n \equiv 1 \pmod{p},$$

nella maniera seguente:

$$(B) \qquad \left\{ \begin{array}{llll} 1, & \gamma_1, & \gamma_2, \cdots, & \gamma_{n-1}, \\ a_1, & a_1\gamma_1, & a_1\gamma_2, \cdots, & a_1\gamma_{n-1}, \\ a_2, & a_2\gamma_1, & a_2\gamma_2, \cdots, & a_2\gamma_{n-1}, \\ \cdots & \cdots & \cdots & \cdots \\ a_{\frac{p-1}{n}-1}, & a_{\frac{p-1}{n}-1}\gamma_1, & a_{\frac{p-1}{n}-1}\gamma_2, \cdots, & a_{\frac{p-1}{n}-1}\gamma_{n-1}. \end{array} \right.$$

È chiaro che per ottenere un sistema completo di n^{imo} grado basterà scegliere un numero e uno solo di ciascuna riga del quadro B. Ne risulta anche che *in un sistema completo di resti (mod. p), esistono $n^{\frac{p-1}{n}}$ sistemi completi di n^{imo} grado.*

Per $n = 2$, risulta subito che *i numeri*

$$(C) \qquad 1, 2, 3, \cdots, \frac{p-1}{2}$$

formano un sistema completo di 2° grado, qualunque sia p.

3. Qual parte rappresentino i numeri di un sistema completo di n^{imo} grado nella risoluzione delle congruenze binomie di grado n, apparisce subito dal seguente teorema fondamentale:

Se i numeri

$$(D) \qquad r_1, r_2, \cdots, r_{\frac{p-1}{n}}$$

formano un sistema completo di n^{imo} grado (mod. p), posto

$$(5) \qquad A_k \equiv -n\left(r_1^{nk-1} + r_2^{nk-1} + \cdots + r_{\frac{p-1}{n}}^{nk-1}\right) \pmod{p},$$

il polinomio

$$A_0 + A_1 a + A_2 a^2 + \cdots + A_{\frac{p-1}{n}-1} a^{\frac{p-1}{n}-1} \tag{6}$$

è una soluzione apiristica della congruenza binomia (1). *Inoltre, per ogni a residuo n-ico di p, esso è congruo all' associato*) di quel numero del sistema* (D) *che soddisfa alla congruenza*

$$x^n \equiv \frac{1}{a} \pmod{p}.$$

Sia r_0 quel numero del sistema (D) che verifica la (1) e poniamo

$$x_0 \equiv \sum_{k=0}^{\frac{p-1}{n}-1} A_k a^k \pmod{p}.$$

Per l'ipotesi (5) si ha

$$x_0 \equiv -n \sum_{k=0}^{\frac{p-1}{n}-1} r_0^{nk} \sum_{h=1}^{\frac{p-1}{n}} r_h^{nk-1} \equiv -n \sum_{h=1}^{\frac{p-1}{n}} \frac{1}{r_h} \sum_{k=0}^{\frac{p-1}{n}-1} (r_0 r_h)^{nk}$$

$$\equiv -n \sum_{h=1}^{\frac{p-1}{n}} \frac{1}{r_h} \frac{(r_0 r_h)^{p-1} - 1}{(r_0 r_h)^n - 1}. \tag{7}$$

Quando h percorre il sistema degl' indici $1, 2, 3, \cdots, \frac{p-1}{n}$, il prodotto $r_0 r_h$ percorre un sistema completo di n^{imo} grado, e incontrerà quindi uno e un sol numero h_0 tale che sia

$$(r_0 r_{h_0})^n \equiv 1 \pmod{p}.$$

Per tal valore h_0 si ha

$$r_{h_0}^n \equiv \frac{1}{a}, \quad \frac{(r_0 r_{h_0})^{p-1} - 1}{(r_0 r_{h_0})^n - 1} \equiv \frac{p-1}{n} \pmod{p},$$

mentre i termini della somma (7), corrispondenti agli altri valori di h, sono divisibili per p, onde si ottiene

$$x_0 \equiv \frac{1}{r_{h_0}} \pmod{p}.$$

Innalzando ambo i membri di questa congruenza a potenza n^{ima}, si ottiene

$$x_0^n \equiv a \pmod{p}.$$

Il teorema è dunque dimostrato.

---

*) Due numeri α, α_1 si dicono *associati* (*mod. p*), quando sia $\alpha\alpha_1 \equiv 1 \pmod{p}$. L'associato di un numero $\alpha \not\equiv 0 \pmod{p}$ si indica anche con $\frac{1}{\alpha}$ (Gauss).

4. Per $n = 2$, indicando con s_r la somma delle potenze r^{ime} dei numeri del sistema (C), si ottiene la seguente soluzione apiristica della congruenza binomia quadratica:

$$(8) \quad x_0 \equiv -2\left(s_{-1} + s_1 a + s_3 a^2 + s_5 a^3 + \cdots + s_{p-4} a^{\frac{p-3}{2}}\right) \pmod{p}.$$

Se poi s'introducono i numeri B_r di Bernoulli, definiti dall' eguaglianza simbolica

$$(B+1)^r - B^r = r,$$

osservando che, per note proprietà di questi numeri, si ha

$$1^r + 2^r + \cdots + \left(\frac{p-1}{2}\right)^r \equiv -2\left(1 - \frac{1}{2^{r+1}}\right)\frac{B_{r+1}}{r+1} \pmod{p},$$

la (8) si esprimerà in modo elegante, ed introducendo i numeri di Genocchi $G_r = (2^r - 1)B_r$, i quali sono interi, si potrà dire in forma concisa *che lo sviluppo simbolico secondo le potenze di* $\sqrt{a}$ *dell' espressione*

$$4 \log\left(1 - \tfrac{1}{2} G \sqrt{a}\right) + \sqrt{a},$$

arrestato alla potenza di esponente $p - 1$, *è una soluzione apiristica della congruenza binomia quadratica.*

5. Col teorema del n. 3 si può dire risoluta la questione di trovare una soluzione apiristica di una congruenza binomia, anzi, potendo ricondursi la risoluzione di una congruenza binomia qualunque a quella di congruenze binomie di grado primo, può anche dirsi che per risolvere col nostro metodo una congruenza binomia qualunque *non occorrono tentativi.* Difatti, quando n è primo, le soluzioni della congruenza (4), che servono alla costruzione di un sistema completo di n^{imo} grado, sono tutte, tranne quelle congrue a 1, le soluzioni della congruenza

$$x^{n-1} + x^{n-2} + \cdots + x + 1 \equiv 0 \pmod{p},$$

che è riducibile a congruenze binomie di grado inferiore a n.

In pratica però il metodo riesce assai lungo e faticoso. Converrà invece applicare le speciali formole di risoluzione dei nn. seguenti assai più semplici nella forma, e sottomettersi alla determinazione per tentativi di alcuni elementi che in dette formole si trovano.

6. È facile dimostrare che, *decomposto* $p - 1$ *in due fattori primi tra loro* m *e* $\frac{p-1}{m}$, *il primo dei quali sia multiplo di* n, *se* γ *e* δ *sono due numeri appartenenti rispettivamente agli esponenti* m *e* $\frac{p-1}{m}$ *secondo il modolo* p, *i numeri*

$$\gamma^r \delta^s, \quad \begin{cases} r = 0, 1, 2, \cdots, \frac{m}{n} - 1, \\ s = 0, 1, 2, \cdots, \frac{p-1}{n} - 1 \end{cases}$$

formano un sistema completo di n^{imo} grado.

Applicando allora il teorema del n. 3, si può porre

$$A_k \equiv -n \sum_{r=0}^{\frac{m}{n}-1} \sum_{s=0}^{\frac{p-1}{m}-1} (\gamma^r \delta^s)^{nk-1} \equiv -n \frac{\gamma^{(nk-1)\frac{m}{n}} - 1}{\gamma^{nk} - 1} \cdot \frac{\delta^{\frac{p-1}{m}(nk-1)} - 1}{\delta^{nk} - 1} \pmod{p},$$

donde segue, se è $nk \equiv 1 \pmod{\frac{p-1}{m}}$:

$$A_k \equiv -n \frac{p-1}{m} \frac{\gamma^{(nk-1)\frac{m}{n}} - 1}{\gamma^{nk-1} - 1} \pmod{p},$$

e se non è $nk \equiv 1 \pmod{\frac{p-1}{m}}$:

$$A_k \equiv 0 \pmod{p}.$$

Ne risulta che *se μ è una soluzione della congruenza*

$$nk \equiv 1 \pmod{\frac{p-1}{m}},$$

l'espressione

$$(9) \qquad -\frac{n}{m} \alpha^{\mu} \left(\gamma^{\frac{m}{n}} - 1\right) \sum_{s=0}^{\frac{m}{n}-1} \frac{\alpha^{s\frac{p-1}{m}}}{\gamma^{\left(\mu + s\frac{p-1}{m}\right)n-1} - 1}$$

è una soluzione apiristica della congruenza binomia di n^{imo} grado.

Per applicare la (9) non occorre che la conoscenza di γ. Giova poi osservare che essendo

$$1, \gamma^{\frac{m}{n}}, \gamma^{2\frac{m}{n}}, \cdots, \gamma^{(n-1)\frac{m}{n}}$$

un sistema completo di soluzioni apiristiche della congruenza $x^n \equiv 1 \pmod{p}$, da una soluzione della congruenza (1) potrà dedursi un sistema completo di soluzioni di essa.

Se n è primo con $\frac{p-1}{n}$, si può assumere $m = n$, e dalla (9) si deduce il risultato noto che se *n è primo con $\frac{p-1}{n}$, è a^{μ} una soluzione apiristica della congruenza $x^n \equiv a \pmod{p}$.*

Se si assume $m = p - 1$, e quindi $\mu = 0$, si dedurrà dalla (9) che *se g è una radice primitiva di p, una soluzione apiristica della congruenza binomia di n^{imo} grado è*

$$n\left(g^{\frac{p-1}{n}} - 1\right) \sum_{s=0}^{\frac{p-1}{n}-1} \frac{a^s}{g^{ns-1} - 1}.$$

7. L'espressione (9) può essere tuttavia semplificata nella forma quando si osservi che esiste sempre un numero γ_1 appartenente all' esponente m (mod. p), che verifichi la congruenza

$$x^{\frac{p-1}{m}} \equiv \gamma \pmod{p}.$$

Allora, mutando γ in γ_1 nella (9), e notando che, posto

$$\mu n - 1 = \nu \frac{p-1}{m},$$

si ha

$$\gamma_1^{\left(\mu + s\frac{p-1}{m}\right)n-1} \equiv \gamma^{\nu+sn}, \quad \gamma^{\frac{m}{n}} \equiv \gamma^{-\nu\frac{m}{n}} \pmod{p},$$

risulta dalla (9) quest' altra soluzione apiristica della congruenza binomia di n^{imo} grado

$$\frac{n}{m} a^{\mu}\left(\gamma^{\nu\frac{m}{n}} - 1\right) \sum_{s=0}^{\frac{m}{n}-1} \frac{a^{s\frac{p-1}{m}}}{\gamma^{\nu+sn} - 1}. \tag{10}$$

8. La risoluzione di una congruenza binomia di grado n, (mod. p), si può sempre ridurre alla risoluzione di congruenze binomie di grado primo. Ora se n è un numero primo ed n^r la massima potenza di n, che divide $p - 1$, essendo ω un non residuo n-ico qualunque di p, si può assumere $\gamma \equiv \omega^{\frac{p-1}{n^r}} \pmod{p}$.

La determinazione di un numero ω non presenta difficoltà in pratica.

In particolare, per $n = 2$, si ottiene che *se ω è un non residuo quadratico di p, una soluzione apiristica della congruenza binomia quadratica è*

$$\frac{1}{2^{r-2}} a^{\frac{p+2^r-1}{2^{r+1}}} \sum_{s=0}^{2^{r-1}} \frac{a^{s\frac{p-1}{2^r}}}{\omega^{(2s+1)\frac{p-1}{2^r}} - 1}. \tag{11}$$

Per esempio, se p è della forma $8m + 5$, si può assumere $\omega = 2$, e però *una soluzione apiristica della congruenza binomia quadratica, secondo un modulo p della forma $8m + 5$, è*

$$\frac{1}{2} a^{\frac{p+3}{8}} \left[2^{\frac{p-1}{4}} + 1 - \left(2^{\frac{p-1}{4}} - 1\right) a^{\frac{p-1}{4}}\right]. \tag{12}$$

9. In pratica, per la determinazione delle soluzioni minime positive (radici) della congruenza binomia, converrà assumere per m il minimo valore possibile, cioè il prodotto delle potenze dei fattori primi di n, con quell' esponente col quale entrano in $p-1$. Se $u, v, w, \cdots$ sono i diversi fattori primi di n, i quali entrano in $p-1$ alle potenze di grado $r, s, t, \cdots$ rispettivamente, si determineranno i numeri $\omega_u, \omega_v, \omega_w, \cdots$ rispettivamente non residui u-ico, v-ico, w-ico, $\cdots$ di p, e si assumerà

$$\gamma \equiv \omega_u^{\frac{p-1}{u^r}} \cdot \omega_v^{\frac{p-1}{v^s}} \cdot \omega_w^{\frac{p-1}{w^t}}, \cdots \pmod{p}.$$

Posto poi

$$a^{\frac{p-1}{m}} \equiv A, \quad \gamma^\nu - 1 \equiv M_0, \quad \gamma^n \equiv N, \quad M_s \equiv \gamma^{\nu+sn} - 1 \pmod{p},$$

i numeri M_s si otterranno con la relazione ricorrente

$$M_s \equiv N(M_{s-1} + 1) - 1 \pmod{p}.$$

Indicando poi con M il minimo comune multiplo dei numeri

$$M_0, M_1, M_2, \cdots, M_{\frac{m}{n}-1},$$

e con $\overline{M}$ l'associato di M secondo il modolo p, posto

$$U_r \equiv \frac{M}{M_r}\overline{M},$$

la (10) assumerà la forma

$$\frac{n}{m} a^\mu \left[(M_0+1)^{\frac{m}{n}} - 1\right] \sum_{s=0}^{\frac{m}{n}-1} A^s U_s,$$

dalla quale si otterranno le soluzioni minime positive con facile calcolo.

10. Per applicare il metodo ad un esempio, determiniamo una soluzione apiristica della congruenza

$$x^3 \equiv a \pmod{73}.$$

Possiamo assumere $m = 9$, $\mu = 3$, $\nu = 1$. Un non residuo cubico di 73 è 2. Infatti si ha

$$2^3 \equiv 8, \quad 2^6 \equiv -9, \quad 2^9 \equiv -72 \equiv 1, \quad 2^{12} \equiv 8, \quad 2^{24} \equiv -9 \pmod{73}.$$

Possiamo quindi porre

$$\gamma \equiv 2^8 \equiv 37 \pmod{73}.$$

Intanto si ha

$$N \equiv 2^{24} \equiv -9,$$

$$M_0 \equiv \gamma^\nu - 1 \equiv 2^8 - 1 \equiv 36, \quad M_1 \equiv -9 \cdot 37 - 1 \equiv -42,$$

$$M_2 \equiv 9 \cdot 41 - 1 \equiv 3 \pmod{73}.$$

Il minimo comune multiplo dei numeri 36, 42, 3 è $M = 252$ e il suo associato è congruo a 31 (mod. 73). Onde si ha

$$U_0 \equiv \frac{M}{M_0}\overline{M} \equiv 7 \cdot 31 \equiv -2, \qquad U_1 \equiv \frac{M}{M_1}\overline{M} \equiv -6 \cdot 31 \equiv 33,$$

$$U_2 \equiv \frac{M}{M_2}\overline{M} \equiv -24 \pmod{73}.$$

Adunque una soluzione apiristica della congruenza data è

$$21a^3(-2 + 33a^8 - 24a^{16}).$$

Per $a = 7$, essendo 7 un residuo cubico di 73, questa espressione, dà subito come radice della congruenza $x^3 \equiv 7 \pmod{73}$, il numero 13. Le altre due radici si ottengono prendendo i resti (mod. 73) dei prodotti di questo numero per $\gamma^{\frac{m}{n}} \equiv 2^{24} \equiv -9$, e per $\gamma^{2\frac{m}{n}} \equiv 8$: esse sono 29 e 31.

Palermo, marzo 1906.