LA RISOLUZIONE APIRISTICA DELLE CONGRUENZE BINOMIE E LA FORMULA DI INTERPOLAZIONE DI LAGRANGE (*)

Alla risoluzione *apiristica* di una congruenza binomia il prof. CIPOLLA ha dedicato tutta una serie di Note interessanti (1), il cui risultato centrale è il seguente (2):

Se p è un numero primo, n è un divisore di $p-1$ ed $r_1, r_2, \dots, r_{\frac{p-1}{n}}$ è un sistema completo di n^{esimo} grado (mod. p), *posto*

$$A_h \equiv -n\left(r_1^{nh-1} + r_2^{nh-1} + \dots + r_{\frac{p-1}{n}}^{nh-1}\right) \pmod{p} \tag{1}$$

il polinomio

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

per ogni a residuo n.ico di p fornisce una soluzione della congruenza binomia

$$x^n \equiv a \pmod{p}. \tag{3}$$

La dimostrazione di questo teorema indicata dal prof. CIPOLLA, consistendo nel verificare che la (2), sotto l'ipotesi (1), fornisce real-

(*) *Rend. Reale Accad. dei Lincei*, (6) 3 (1926), pp. 390-394.

(1) M. CIPOLLA: *a*) *Formole di risoluzione della congruenza binomia quadratica e biquadratica* (« Rendic. della R. Accad. delle Scienze fis. e mat. di Napoli », gennaio 1905); *b*) *Sulla risoluzione apiristica delle congruenze binomie secondo un modulo primo* (« Math. Ann. », Bd. LXIII, 1906); *c*) *Sulla risoluzione apiristica delle congruenze binomie*, Note 1ª e 2ª (*Rend. R. Acc. Lincei*, fasc. 8° e 9° del vol. XVI della serie 5ª, 1° semestre 1907).

(2) Cfr. loc. cit., (1) *b*), n. 3.

mente una soluzione della (3), non dà affatto ragione della struttura della formula (1).

Mi pare pertanto che valga la pena di far vedere come al teorema del prof. CIPOLLA si possa pervenire in maniera da rendere esatto conto del perchè i coefficienti del polinomio (2) debbano esser definiti da una formula del tipo (1).

Per questo, atteso che una congruenza, rispetto a un numero primo (o, più generalmente, rispetto ad un ideale primo) come modulo, è niente altro che un'*equazione* nel corpo numerico (finito) costituito da un qualsiasi sistema completo di resti rispetto al modulo, mi varrò in quanto segue del linguaggio della teoria dei corpi numerici [3]; e per la chiarezza dell'esposizione non tralascerò di richiamare rapidamente nel n. 1 i semplici e ben noti principii sui quali è fondato il procedimento.

1. Detto n un intero positivo, un numero non nullo a di un corpo numerico si dice, come è noto, una *potenza* n^{esima}, se è possibile determinare nel corpo un numero (non nullo) α, per il quale si abbia $a = \alpha^n$.

Ciò posto sia C un corpo numerico finito con N elementi (sì che per N sussisterà un'eguaglianza della forma $N = p^m$, con p numero primo).

Si dimostra subito che:

Indicato con δ il massimo comune divisore di n ed $N-1$, in C non esistono che $\frac{N-1}{\delta}$ potenze n^{esime};

e che:

Ognuna di queste è potenza n^{esima} di δ numeri di C.

Infatti sia ϱ un numero primitivo [4] di C, di guisa che i numeri non nulli di C saranno dati da

$$\varrho, \varrho^2, \varrho^3, \ldots, \varrho^{N-1} = 1.$$

Fra questi ϱ^h sarà una potenza n^{esima}, se, e solo se, esiste nella serie $1, 2, \ldots, N-1$ un intero x per il quale si abbia

$$(\varrho^x)^n = \varrho^{nx} = \varrho^h,$$

[3] Per la teoria generale dei corpi numerici vedi ad es. G. SCORZA, *Corpi numerici e algebre* (Messina, Principato, 1921).

[4] Cfr. loc. cit. (3), p. 123.

ossia

$$nx \equiv h \qquad (\text{mod. } N-1).$$

Ora questa congruenza ammette soluzioni, se, e solo se, h è divisibile per δ; e in caso che h sia divisibile per δ, ammette δ soluzioni incongrue; dunque, posto

$$t = \frac{N-1}{\delta},$$

le potenze n^{esime} di C sono

$$a_1 = \varrho^{\delta}, a_2 = \varrho^{2\delta}, \dots, a_t = \varrho^{t\delta}$$

e ciascuna di esse è potenza n^{esima} di δ numeri di C.

Con ciò le due affermazioni fatte sono dimostrate.

Da

$$a_j = \varrho^{j\delta} \qquad (j = 1, \dots, t)$$

segue

$$a_j^t = \varrho^{j\delta t} = \varrho^{j(N-1)} = (\varrho^{N-1})^j = 1;$$

dunque:

Un numero di C è potenza n^{esima} quando, e solo quando, è radice della equazione

(4) $$x^t - 1 = 0.$$

2. E adesso si consideri in C l'equazione binomia

(5) $$x^n - a = 0,$$

con $a \neq 0$, la quale naturalmente sarà priva di radici o ne avrà δ, secondo che a non è od è una potenza n^{esima}.

Risolverla *apiristicamente* significa costruire un polinomio in C di grado $\leq t-1$

(6) $$f(x) = A_0 + A_1 x + A_2 x^2 + \dots + A_{t-1} x^{t-1},$$

tale che per ogni a potenza n^{esima} di C $f(a)$ risulti una radice dell'equazione (5).

Evidentemente, mantenuti per le $a_1, a_2, \dots, a_t$ i significati già chiariti, il polinomio $f(x)$ soddisfa alla condizione voluta, se, e solo se, è

(7) $$f(a_1) = r_1, \quad f(a_2) = r_2, \dots, f(a_t) = r_t,$$

essendo r_j uno qualunque dei δ numeri la cui potenza n^{esima} è a_j $(j = 1, \dots, t)$.

Ora, fissati i numeri $r_1, r_2, \dots, r_t$, le (7) individuano univocamente $f(x)$; e il sistema di numeri $r_1, r_2, \dots, r_t$ può fissarsi in δ^t modi differenti, dunque:

L'equazione binomia (5) *è risolubile apiristicamente; di polinomi atti a risolverla in siffatta maniera ne esistono*

$$\delta^{\frac{N-1}{\delta}}$$

e la determinazione di tali polinomi non è che un problema di interpolazione.

3. Passiamo adesso alla costruzione effettiva del polinomio (6) per il quale sussistono le (7).

Il polinomio $f(x)$ di grado $\leq t-1$, che soddisfa alle condizioni (7), può essere espresso intanto nella forma classica Lagrangiana

$$f(x) = \sum_j^{1\dots t} r_j \frac{(x-a_1)(x-a_2)\dots(x-a_{j-1})(x-a_{j+1})\dots(x-a_t)}{(a_j-a_1)(a_j-a_2)\dots(a_j-a_{j-1})(a_j-a_{j+1})\dots(a_j-a_t)},$$

ossia

$$f(x) = \sum_j^{1\dots t} r_j \frac{\varphi(x)}{\varphi'(a_j)(x-a_j)},$$

ove si ponga

$$\varphi(x) = (x-a_1)(x-a_2)\dots(x-a_t),$$

e con $\varphi'(x)$ si indichi la derivata di $\varphi(x)$ [5].

Ora, giacchè $a_1, a_2, \dots, a_t$, per quanto più sopra è stato detto, sono le radici della (4), è

$$\varphi(x) = x^t - 1,$$

indi

$$\frac{\varphi(x)}{x-a_j} = \sum_h^{0\dots t-1} a_j^{t-h-1} x^h = \sum_h^{0\dots t-1} r_j^{n(t-h-1)} x^h,$$

e

$$\varphi'(a_j) = t a_j^{t-1} = t r_j^{n(t-1)}, \tag{8}$$

[5] Cfr. loc. cit., (3), p. 161.

dunque resta

$$f(x) = \frac{1}{t} \sum_{j}^{1\ldots t} \sum_{h}^{0\ldots t-1} r_j^{1-nh} x^h; \tag{9}$$

cioè il polinomio (6) soddisfa alle condizioni (7) quando, e solo quando, è

$$A_h = \frac{1}{t} \sum_{j}^{1\ldots t} r_j^{1-nh}. \tag{10}$$

Avvertasi che perchè nella (8) il fattore t e nelle (9) e (10) il fattore $\frac{1}{t}$ siano, come di dovere, numeri di C, bisogna pensare t non come simbolo di numero intero, ma come simbolo di un conveniente numero di C, a norma di una ben nota convenzione (6).

Secondo tale convenzione *in* C si ha $p = 0$ indi $N = 0$; per conseguenza *in* C si può porre

$$t = -\frac{1}{\delta},$$

e la (10) diventa

$$A_h = -\delta \sum_{j}^{1\ldots t} r_j^{1-nh}. \tag{11}$$

4. Se t numeri di C godono della proprietà che le loro potenze n^{esime} danno tutte le potenze n^{esime} di C, della medesima proprietà godono evidentemente i loro reciproci; ma cambiando r_j in $\frac{1}{r_j}$ la (11) diventa

$$A_h = -\delta \sum_{j}^{1\ldots t} r_j^{nh-1}, \tag{12}$$

dunque il polinomio (6) è atto a fornire una soluzione apiristica dell'equazione (5) anche quando i coefficienti A_h vi si intendano definiti dalla (12).

Ora la (12) equivale alla (1) del prof. CIPOLLA, quando si supponga che sia $N = p$, che n sia un divisore di $p - 1$ e che C sia il corpo numerico costituito da un sistema completo di resti rispetto al modulo p.

(6) Cfr. loc. cit., (5).