ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCCIV.

1907

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XVI.

1° SEMESTRE.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1907

Matematica. — *Sulla risoluzione apiristica delle congruenze binomie.* Nota 2ª di MICHELE CIPOLLA, presentata dal Corrispondente A. VENTURI.

In una precedente Nota di egual titolo, noi ci occupammo della risoluzione apiristica di una congruenza binomia, di cui il grado e il modulo sono potenze di uno stesso numero primo.

Qui vogliamo considerare il caso generale di una congruenza binomia di grado n, secondo il modulo p^m, essendo p un numero primo dispari ed n un divisore qualunque di $p^{m-1}(p-1)$.

Questo caso richiede la considerazione dei cosiddetti *sistemi completi* n^{imo} *grado* (*mod.* p^m); il quale concetto, estensione di quello introdotto per la prima volta da noi nella risoluzione apiristica delle congruenze binomie secondo un modulo primo, ci condurrà alla ripartizione dei numeri di un sistema completo di resti (mod. p^m) in altri sistemi, in ciascuno dei quali esiste uno ed un sol numero che sia soluzione di una data congruenza binomia (mod. p^m). Dopo ciò non sarà difficile giungere alle cercate formole di risoluzione.

§ 1. — *Sistemi completi di* n^{imo} *grado* (*mod.* p^m).

1. Se i numeri

$$r_1, r_2, \dots, r_k \tag{1}$$

sono primi con p e le loro potenze n^{ime} sono incongrue fra loro (mod. p^m) e inoltre formano un gruppo secondo il modulo p^m stesso, noi diremo che essi costituiscono *un sistema completo di* n^{imo} *grado* (*mod.* p^m), *d'ordine* k.

L'ordine k è un divisore di $\frac{p^{m-1}(p-1)}{n}$, poichè il gruppo corrispondente delle potenze n^{ime} è un divisore del gruppo d'ordine $\frac{p^{m-1}(p-1)}{n}$, formato da tutti i residui n-ici di p^m, incongrui fra loro (mod. p^m).

Le potenze n^{ime} *dei numeri* (1) *sono tutte le soluzioni della congruenza*

$$x^k \equiv 1 \quad (\text{mod. } p^m). \tag{2}$$

Infatti, se μ è il periodo di r_i^n, p. es., sarà μ un divisore di k, onde r_i^n è una soluzione della congruenza $x^\mu \equiv 1$ (mod. p^m), e però della (2). Tutte le potenze n^{ime} dei numeri (1), soddisfacendo alla congruenza (2) ed essendo incongrue fra loro (mod. p^m) e in numero di k, son tutte le soluzioni della (2).

Se $\gamma_1, \gamma_2, \dots, \gamma_n$ sono tutte le soluzioni della congruenza $x^n \equiv 1$ (mod. γ^m), i numeri $r_i \gamma_n$ $(i = 1, 2, \dots, k\ ;\ h = 1, 2, \dots n)$ si possono ripartire nei sistemi

$$(3) \qquad \begin{cases} r_1\gamma_1\ ,\ r_1\gamma_2\ ,\ \dots\ ,\ r_1\gamma_n \\ r_2\gamma_1\ ,\ r_2\gamma_2\ ,\ \dots\ ,\ r_2\gamma_n \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ r_k\gamma_1\ ,\ r_k\gamma_2\ ,\ \dots\ ,\ r_k\gamma_n\,. \end{cases}$$

È chiaro che un sistema completo di n^{tmo} grado (mod. p^m) contiene uno ed un sol numero di ciascun sistema del quadro (3), onde *coi* $\varphi(p^m)$ *numeri di un sistema completo di resti primi con* p, *secondo il mod.* p^m, *si possono formare* n^k *sistemi completi di* n^{imo} *grado* (*mod.* p^m), *d'ordine* k.

2. Sia

$$(4) \qquad R_1\ ,\ R_2\ ,\ \dots\ ,\ R_k$$

un gruppo di residui n-ici (un sistema completo di n^{imo} grado) secondo il mod. p^m, d'ordine k; si può facilmente dimostrare che *se* k *è divisibile per* p^r $(r \leq m-1)$ *ed* s *è un numero intero non superiore ad* r *i numeri* (4) *si possono ripartire in* p^s *gruppi di residui* n-ici (*sistemi completi di* n^{imo} *grado*) *secondo il mod.* p^{m-s}, *tutti dell'ordine* $\frac{k}{p^s}$; *e se invece* k *non è divisibile per* p, *ma è un divisore di* $\frac{1}{n}p^{m-r-1}(p-1)$ *il gruppo* (*il sistema*) (3) *è anche un gruppo di residui* n-ici (*un sistema di* n^{imo} *grado*) *secondo il mod.* p^{m-r}.

Tralasceremo per brevità le dimostrazioni di questi teoremi, che si fondano del resto sui più elementari concetti della teoria generale dei gruppi e della teoria delle congruenze.

3. *Se* k *non è divisibile per* p *e i numeri*

$$(4) \qquad S_1\ ,\ S_2\ ,\ \dots\ ,\ S_k$$

formano un gruppo di residui n-*ici, secondo il mod.* p^{m-r}, *i numeri*

$$(5) \qquad S_1^{p^r}\ ,\ S_2^{p^r}\ ,\ \dots\ ,\ S_k^{p^r}$$

formeranno un gruppo di residui n-ici *secondo il mod.* p^m.

Infatti i numeri (4) sono tutte le soluzioni della congruenza $x^k \equiv 1$ (mod. p^{m-r}), e però tutti i numeri (5), che sono incongrui fra loro (mod. p^m), sono le soluzioni della congruenze $x^k \equiv 1$ (mod. p^m), e quindi formano un gruppo di residui n-ici secondo il mod. p^m.

4. Un gruppo di residui n-ici (mod. p^m) lo diremo *proprio*, quando due numeri qualunque di esso non sono mai congrui fra loro secondo il mod. p^m. Così pure si dirà che i numeri di un sistema completo di n^{imo} grado

(mod. p^m) formano un sistema *proprio* quando le loro potenze n^{imo} formano un gruppo proprio.

Dai teoremi dei nn. 2 e 3 risulta subito che *condizione necessaria e sufficiente perchè un sistema completo di n^{imo} grado (un gruppo di residui n-ici) sia proprio è che il suo ordine k non sia divisibile per p.* Inoltre *se*

$$\varrho_1 , \varrho_2 , \dots , \varrho_k \tag{6}$$

è un sistema completo e proprio di n^{imo} grado (mod. p^m), si può porre

$$\varrho_i \equiv r_i^{p^{m-1}} \pmod{p^m}, \qquad (i = 1 , 2 , \dots k), \tag{7}$$

essendo

$$r_1 , r_2 , \dots , r_k$$

un sistema completo di n^{imo} grado secondo il mod. p.

5. Ciò posto, sia ν un divisore di $p-1$, e $k = \frac{p-1}{\nu}$, siano inoltre

$$t_1 , t_2 , \dots , t_{p^{m-1}}$$

tutte le soluzioni della congruenza

$$x^{p^{m-1}} \equiv 1 \pmod{p^m} \tag{8}$$

e formiamo il quadro

$$\begin{cases} t_1 \varrho_1 & , t_1 \varrho_2 & , \dots , t_1 \varrho_k \\ t_2 \varrho_1 & , t_2 \varrho_2 & , \dots , t_2 \varrho_k \\ \cdot & \cdot & \cdot \\ t_{p^{m-1}} \varrho_1 & , t_{p^{m-1}} \varrho_2 & , \dots , t_{p^{m-1}} \varrho_k . \end{cases} \tag{9}$$

È facile vedere che in questo quadro sono distribuiti in p^{m-1} sistemi i numeri di un sistema completo di ν^{imo} grado (mod. p^m), le cui potenze ν^{ime} sono *tutti* i residui ν-*ici* di p^m, primi con p. È importante poi osservare che se *a è un residuo ν-ico di p^m*, vi è nel quadro (9) un sistema solo che ammetta una soluzione (e una soltanto) della congruenza

$$x^\nu \equiv a \pmod{p^m}. \tag{10}$$

Infatti si scorge subito che il numero

$$t_0 \equiv a^{\frac{p^m - 2p^{m-1} + 1}{\nu}} \pmod{p^m},$$

è una soluzione della (8); sia ora r_0 quel numero del sistema (9), che verifica la congruenza $x^\nu \equiv a$ (mod. p), si avrà

$$r_0^{p^{m-1}\nu} \equiv a^{p^{m-1}} \pmod{p^m}$$

cioè, posto $\varrho_0 \equiv r_0^{p^{m-1}}$ (mod. p^m),

$$\varrho_0^\nu \equiv a^{p^{m-1}} \pmod{p^m} \tag{11}$$

e quindi

$$(t_0 \varrho_0)^\nu \equiv a^{p^m - 2p^{m-1}+1} \equiv a \pmod{p^m}.$$

Premesso ciò, si è condotti facilmente alla determinazione di una soluzione apiristica di una congruenza (10), come vedremo nei successivi §§.

§ 2. — *Risoluzione di una congruenza binomia (mod. p^m), il cui grado è un divisore di $p-1$.*

6. In vista di ulteriori applicazioni noi dimostreremo il seguente teorema più generale:

Se i numeri

$$\varrho_1, \varrho_2, \dots, \varrho_{\frac{p-1}{\nu}} \tag{12}$$

formano un sistema completo e proprio di ν^{imo} grado secondo il mod p^m, posto

$$A_k \equiv \sum_{i=1}^{\frac{p-1}{\nu}} \varrho_i^{\nu k - \alpha}, \tag{13}$$

dove α è un numero intero, l'espressione

$$\frac{\nu}{p-1} a^{\frac{p^m - 2p^{m-1}+1}{\nu}\alpha} \sum_{k=0}^{\frac{p-1}{\nu}-1} A_k a^{kp^{m-1}} \tag{14}$$

è congrua (mod. p^m) alla potenza α^{ima} di una soluzione apiristica della (10).

Infatti, indicando con x_α l'espressione (14) e con ϱ_0 quel numero del sistema (6), che soddisfa alla congruenza $x^\nu \equiv a^{m-1}$ (mod. p^m) [cfr. n. 5, formola (11)], la (14) si può mettere sotto la forma

$$x_\alpha \equiv \frac{\nu}{p-1} a^{\frac{p^m - 2p^{m-1}+1}{\nu}\alpha} \sum_{i=1}^{\frac{p-1}{\nu}} \frac{(\varrho_0 \varrho_i)^{p-1} - 1}{(\varrho_0 \varrho_i)^\nu - 1} \cdot \varrho_i^{-\alpha}. \tag{15}$$

Ora si osservi che, quando i assume i valori $1, 2, \dots, \frac{p-1}{\nu}$, $(\varrho_0 \varrho_i)^\nu$ percorre un gruppo proprio di residui ν-ici (mod. p^m), onde la differenza $(\varrho_0 \varrho_i)^\nu - 1$ per un solo valore i_0 di i sarà divisibile per p^m.

Poichè, in virtù delle (7), si ha

$$(\varrho_0 \varrho_i)^{p-1} - 1 \equiv (r_0 r_i)^{p^{m-1}(p-1)} - 1 \equiv 0 \pmod{p^m},$$

tutti i termini della somma che figura nella (15) per $i \neq i_0$ sono divisibili

per p^m; siccome poi per $i = i_0$, per cui si ha $(\varrho_0 \varrho_{i_0})^\nu - 1 \equiv 0 \pmod{p^m}$ ossia

$$\varrho_{i_0}^\nu \equiv \varrho_0^{-\nu} \pmod{p^m}, \tag{16}$$

risulta

$$\frac{(\varrho_0 \varrho_{i_0})^{p-1} - 1}{(\varrho_0 \varrho_{i_0})^\nu - 1} \equiv \frac{p-1}{\nu} \pmod{p^m},$$

si trae

$$x_\alpha \equiv a^{\frac{p^m - 2p^{m-1}+1}{\nu}\alpha} \varrho_{i_0}^{-\alpha} \pmod{p^m}.$$

Dunque x_α è congruo (mod. p^m) alla potenza α^{ima} del numero

$$a^{\frac{p^m - 2p^{m-1}+1}{\nu}} \varrho_{i_0}^{-1},$$

che è una soluzione della (10), perchè la potenza ν^{ima} di esso, per la (16) e la (11), è congrua ad a (mod. p^m).

Per $\alpha = 1$ si deduce che *l'espressione*

$$\frac{\nu}{p-1} a^{\frac{p^m - 2p^{m-1}+1}{\nu}} \sum_{k=0}^{\frac{p-1}{\nu}-1} A_k a^{p^{m-1}k}, \tag{17}$$

essendo

$$A_k \equiv \sum_{i=1}^{\frac{p-1}{\nu}} \varrho_i^{\nu k - 1}, \tag{18}$$

è una soluzione della congruenza $x^\nu \equiv a$ (*mod.* p^m).

7. Come applicazione di quest'ultimo risultato determiniamo una soluzione apiristica della congruenza

$$x^2 \equiv a \pmod{p^m}. \tag{19}$$

È facile osservare che i numeri

$$1, 2, 3, \ldots, \frac{p-1}{2}$$

costituiscono un sistema completo di 2° grado (mod. p), e però si può porre per tutti i valori di i da 1 a $\frac{p-1}{2}$:

$$\varrho_i \equiv i^{p^{m-1}} \pmod{p^m},$$

onde, posto

$$s_k \equiv \sum_{i=1}^{\frac{p-1}{2}} i^{p^{m-1}(2k-1)} \pmod{p^m},$$

si trae che *l'espressione*

$$\frac{2}{p-1} a^{\frac{p^m-2p^{m-1}+1}{2}} \sum_{k=0}^{\frac{p-1}{2}-1} s_k a^{kp^{m-1}}$$

è una soluzione apiristica della (19).

Si può anche osservare che è, secondo il mod p^m,

$$s_k \equiv \frac{1}{p^{m-1}} \sum_{i=1}^{\frac{p^m-1}{2}} i^{p^{m-1}(2k-1)} \equiv \frac{1}{p^{m-1}} \cdot \frac{\left(\frac{p^m-1}{2}+\mathrm{B}\right)^{p^{m-1}(2k-1)+1} - \mathrm{B}^{p^{m-1}(2k-1)+1}}{p^{m-1}(2k-1)+1},$$

dove le B sono i numeri di Bernoulli, e, in virtù di note proprietà dei polinomi bernoulliani, si ha

$$s_k \equiv -\frac{2}{p^{m-1}\left[p^{m-1}(2k-1)+1\right]}\left(1-\frac{1}{2^{p^{m-1}(2k-1)+1}}\right)\mathrm{B}_{p^{m-1}(2k-1)+1} \pmod{p^m}.$$

Infine, introducendo i numeri di Genocchi $\mathrm{G}_r = (2^r-1)\,\mathrm{B}_r$, che sono interi, si deduce che *l'espressione*

$$(20) \qquad \frac{4}{p^{m-1}(p-1)} \sum_{k=0}^{\frac{p^m-1}{2}} \frac{\mathrm{G}_{p^{m-1}(2k-1)+1}}{2^{p^{m-1}(2k-1)+1}\left[p^{m-1}(2k-1)+1\right]} a^{kp^{m-1}}$$

è una soluzione apiristica della congruenza binomia quadratica.

La formola (20) ha importanza solamente teorica: essa mostra che nel caso di $n=2$ la determinazione dei coefficienti può effettuarsi senza conoscere il numero p.

Formole assai vantaggiose in pratica saranno ottenute nel successivo paragrafo.

§ 3. — *Soluzioni apiristiche ridotte.*

8. La risoluzione di una congruenza binomia di ν^{imo} grado, coi processi esposti nel precedente §, non richiede altro, che la conoscenza di un sistema completo di ν^{imo} grado secondo il mod. p (v. n. 4), per la costruzione del

quale (n. 1) basta la conoscenza delle soluzioni della congruenza $x^\nu \equiv 1$ (mod. p). Poichè la risoluzione di quest'ultima si può ricondurre alla risoluzione di congruenze binomie di grado inferiore, si può anche dire che per risolvere una congruenza binomia qualunque *non occorrono tentativi*. Ma in pratica, specialmente per la determinazione delle soluzioni minime positive (*radici*), il metodo riescirebbe assai faticoso.

Invece si prestan bene in questi casi le così dette *soluzioni apiristiche ridotte*, le quali richiedono la conoscenza di qualche elemento dipendente dal modulo, la cui determinazione per tentativi, del resto, non offre alcuna difficoltà pratica.

9. È facile dimostrare che *decomposto* $p-1$ *in due fattori primi fra loro* μ *e* $\frac{p-1}{\mu}$, *il primo dei quali sia multiplo di* ν, *se* γ *e* δ *sono due numeri appartenenti rispettivamente agli esponenti* μ *e* $\frac{p-1}{\mu}$, *secondo il mod.* p, *i numeri*

$$\gamma^r \delta^s \left(r = 0, 1, 2, \ldots, \frac{\mu}{\nu} - 1 \; ; \; s = 0, 1, 2, \ldots, \frac{p-1}{\nu} - 1 \right),$$

formano un sistema completo di ν^{imo} *grado* (*mod.* p).

Allora, posto

$$\varrho \equiv \gamma^{p^{m-1}} \quad , \quad \pi \equiv \delta^{p^{m-1}} \quad (\text{mod.}\, p),$$

si può nella (14) porre

$$A_k \equiv \sum_{r=0}^{\frac{\mu}{\nu}-1} \sum_{s=0}^{\frac{p-1}{\nu}-1} (\varrho^r \pi^s)^{\nu k - \alpha} \equiv \frac{\varrho^{(\nu k-\alpha)\frac{\mu}{\nu}} - 1}{\varrho^{\nu k - \alpha} - 1} \cdot \frac{\pi^{(\nu k-\alpha)\frac{p-1}{\mu}} - 1}{\pi^{\nu k - \alpha} - 1} \quad (\text{mod.}\, p^m),$$

da cui si trae subito, se non è $\nu k - \alpha \equiv 0 \left(\text{mod.}\, \frac{p-1}{\mu}\right)$,

$$A_k \equiv 0 \quad (\text{mod.}\, p^m),$$

e se invece è $\nu k - \alpha \equiv 0 \left(\text{mod.}\, \frac{p-1}{\mu}\right)$:

$$A_k \equiv \frac{p-1}{\mu} \frac{\varrho^{(\nu k-\alpha)\frac{\mu}{\nu}} - 1}{\varrho^{\nu k - \alpha} - 1} \quad (\text{mod.}\, p^m).$$

Se ne deduce allora che, *se* k_α *è una soluzione della congruenza*

$$(21) \qquad \nu x - \alpha \equiv 0 \quad \left(\text{mod.}\, \frac{p-1}{\mu}\right),$$

l'espressione

$$(22)\qquad -\frac{\nu}{\mu}\, a^{\frac{p^m-2p^{m-1}+1}{\nu}+p^{m-1}k_\alpha}\left(\varrho^{\alpha\frac{\mu}{\nu}}-1\right)\sum_{s=0}^{\frac{\mu}{\nu}-1}\frac{a^{s\frac{p^{m-1}(p-1)}{\mu}}}{\varrho^{\nu\left(k_\alpha+s\frac{p-1}{\mu}\right)}-1}$$

è congrua (mod. p^m) alla potenza α-esima di una soluzione apiristica della (10).

In particolare, per $\alpha=1$, una soluzione apiristica della (10) *è*

$$(23)\qquad -\frac{\nu}{\mu}\, a^{\frac{p^m-2p^{m-1}+1}{\nu}+p^{m-1}k_1}\left(\varrho^{\frac{\mu}{\nu}}-1\right)\sum_{s=0}^{\frac{\mu}{\nu}-1}\frac{a^{s\frac{p^{m-1}(p-1)}{\mu}}}{\varrho^{\nu\left(k_1+s\frac{p-1}{\mu}\right)}-1},$$

dove k_1 è una soluzione della congruenza

$$(24)\qquad \nu x-1\equiv 0\quad\left(\text{mod. }\frac{p-1}{\mu}\right).$$

Se ν è primo con $\frac{p-1}{\nu}$ si può porre $\mu=\nu$, e la (23) allora dà, come soluzione apiristica della (10), l'espressione

$$(25)\qquad a^{\frac{p^m-2p^{m-1}+1}{\nu}+p^{m-1}k_1}.$$

Se si pone $\mu=p-1$, e però $k_\alpha=0$, si ottiene il risultato seguente:

Se g è una radice primitiva di p, l'espressione

$$(26)\qquad -\frac{\nu}{p-1}\, a^{\frac{p^m-2p^{m-1}+1}{\nu}}\left(g^{\frac{p^{m-1}(p-1)}{\nu}\alpha}-1\right)\sum_{s=0}^{\frac{p-1}{\nu}-1}\frac{a^{sp^{m-1}}}{g^{p^{m-1}(\nu s-\alpha)}-1}$$

è congrua alla potenza α^{ima} di una soluzione apiristica della (10).

In particolare, per $\nu=2$ e $\alpha=1$, si ha che l'*espressione*

$$(27)\qquad \frac{4}{p-1}\, a^{\frac{p^m-2p^{m-1}+1}{2}}\sum_{s=0}^{\frac{p-1}{2}-1}\frac{a^{p^{m-1}}}{g^{p^{m-1}(2s-1)}-1}$$

è una soluzione apiristica della congruenza $x^2\equiv a$ (mod. p^m).

10. La (23) può anche mettersi sotto una forma più semplice. A tal fine si osservi che esiste sempre un numero γ_1 appartenente all'esponente μ (mod. p), tale che sia

$$\gamma_1^{\frac{p-1}{\mu}} \equiv \gamma \pmod{p}. \tag{28}$$

Si ponga allora

$$\varrho_1 \equiv \gamma_1^{p^{m-1}} \pmod{p^m} \tag{29}$$

e nella (22) si muti ϱ in ϱ_1. Posto quindi

$$k_\alpha \nu - \alpha = h_\alpha \frac{p-1}{\mu}, \tag{30}$$

e osservando che, per la (28) e la (30), si ha

$$\varrho_1^{\nu\left(k_\alpha + s\frac{p-1}{\mu}\right) - \alpha} \equiv \varrho^{h_\alpha + s\nu} \quad , \quad \varrho_1^{\alpha\frac{\mu}{\nu}} \equiv \varrho^{-h_\alpha \frac{\mu}{\nu}} \pmod{p^m},$$

si ottiene che l'*espressione*

$$-\frac{\nu}{\mu}\, a^{\frac{p^m - 2p^{m-1}+1}{\nu} + p^{m-1}k_\alpha} \left(\varrho^{h_\alpha \frac{\mu}{\nu}} - 1\right) \sum_{s=0}^{\frac{\mu}{\nu}-1} \frac{a^{s\frac{p^{m-1}(p-1)}{\mu}}}{\varrho^{h_\alpha + s\nu} - 1} \tag{31}$$

è congrua (mod. p^m) alla potenza α^{ima} di una soluzione della (10).

Applichiamo la (31) al caso di $n = 2$ e $\alpha = 1$. Se 2^r è la più alta potenza di 2 che divide $p - 1$, si può porre

$$\mu = 2^r \quad , \quad k_1 = \frac{p + 2^r - 1}{2^{r+1}} \quad . \quad h_1 = 1,$$

e poichè, com'è facile osservare, si ha

$$\varrho^{2^{r-1}} \equiv -1 \pmod{p^m},$$

si conclude che l'*espressione*

$$\frac{1}{2^{r-2}}\, a^{\frac{(2^r+1)\,p^{m-1}(p-1)+2^r}{2^{r+1}}} \sum_{s=0}^{2^{r-1}-1} \frac{a^{s\frac{p^{m-1}(p-1)}{2^r}}}{\varrho^{2s+1} - 1} \tag{32}$$

è una soluzione apiristica della congruenza $x^2 \equiv a$ (mod. p^m).

11. Quando si vogliono calcolare le radici di una congruenza binomia qualunque si assumerà per μ il minimo valore possibile, cioè il prodotto dei fattori primi di n, con quell'esponente col quale entrano in $p - 1$.

Se $u, v, w, \ldots$ sono i fattori primi diversi di n, i quali entrano in $p-1$ alle potenze di grado $r, s, t, \ldots$ rispettivamente, si determineranno i numeri $\omega_u, \omega_v, \omega_w, \ldots$ rispettivamente non residui u-ico, v-ico, w-ico, ... di p e si assumerà

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

La determinazione dei numeri ω non presenta difficoltà. Conviene allora calcolare colle formole date nei nn. precedenti, per $m=1$, una radice r della congruenza

$$x^\nu \equiv a \pmod{p};$$

si otterrà allora una radice della (10) calcolando il minimo numero positivo congruo (mod. p^m) al numero

$$a^{\frac{p^m-2p^{m-1}+1}{\nu}} \cdot r^{p^{m-1}}.$$

§ 4. — *Risoluzione di una congruenza binomia (mod. p^m), il cui grado è un divisore qualunque di $p^{m-1}(p-1)$.*

12. Supponiamo ora che il grado n della conguenza

$$x^n \equiv a \pmod{p^m} \tag{33}$$

sia un divisore qualunque di $p^{m-1}(p-1)$, e poniamo $n = p^r \nu$, dove ν è primo con p.

Si possono sempre determinare due numeri interi α e β tali che sia soddisfatta la congruenza

$$\alpha p^r + \nu\beta \equiv 1 \quad [\text{mod. } p^{m-r-1}(p-1)]. \tag{34}$$

Sia y_0 una soluzione della congruenza

$$y^{p^r} \equiv a^\beta \pmod{p^m}$$

e x_1 una soluzione della congruenza

$$x^\nu \equiv a \pmod{p^m},$$

sarà allora $y_0 x_1^\alpha$ una soluzione della (38). Infatti si ha

$$(y_0 x_1^\alpha)^n \equiv y_0^{p^r\nu} \cdot x_2^{\alpha p^r \nu} \equiv a^{\nu\beta+\alpha p^r} \equiv a \pmod{p^m}.$$

Ora si soddisfa alla (34) prendendo

$$\alpha = p^{m-r-1} \quad \text{e} \quad \beta = \frac{p^{m-r} - 2p^{m-r-1} + 1}{\nu}; \tag{35}$$

quindi, moltiplicando una qualunque delle formole ottenute nel § precedente, per $\alpha = p^{m-r-1}$, con la (14) della Nota 1ª, dove sia mutato a in a^β per il valore di β dato dalla (35), si ottiene una soluzione apiristica della congruenza (33).