HIGHER IRREDUCIBLE CONGRUENCES.

BY DR. LEONARD E. DICKSON.

1. Comprising the theory of congruences irreducible modulo p (p=prime), we may establish a theory of quantics belonging to and irreducible in the Galois Field* of order p^n. The existence-proofs of an irreducible congruence modulo p for every degree due to Galois†, Serret‡ and Jordan§ may each be readily generalized to prove that for every m, n and p (=prime) there exists a quantic of degree m belonging to and irreducible in the $GF[p^n]$, or to give a notation, an $IQ[m, p^n]$.

As we may define the $GF[p^{nm}]$ either by an $IQ[m, p^n]$ or by an $IQ[mn, p]$, a theory of the former quantics can often be of practical value in setting up and working in the $GF[p^{nm}]$. In certain investigations (like many due to Jordan), where it seems preferable to use the concrete form of the $GF[p^{nm}]$ (viz., use the quantics built on a Galois imaginary), it may often be simpler, especially if generalizing, to use a defining $IQ[m, p^n]$, keeping the reference $GF[p^n]$ in its abstract form. The quantics then occurring will be of degree $\leqq m-1$ instead of degree $\leqq mn-1$.

The first part of the theory given here runs parallel with the beautiful developments of Serret, Cours D'Algèbre Supérieure, Section III, Chapter III (§360 being a marked exception; compare §16 below), so I content myself with enunciating the more important generalized theorems. As it is quite otherwise with Chapter IV, I give in detail the corresponding developments. The concluding pages in Serret, 199–211 would require a method of attack entirely different (even if capable of generalization).

2. THEOREM. If $F(\xi)$, belonging to and irreducible in the $GF[p^n]$, divides the product $\varphi(\xi) \cdot \chi(\xi)$, it divides one factor at least.

Corollary. The decomposition of a quantic into irreducible factors in the $GF[p^n]$ can be effected in a single way.

3. THEOREM. $F(\xi)$, an $IQ[m, p^n]$, divides the function

* I use the abstract form of the theory due to Galois. See MOORE, Proceedings of the Congress of Mathematics of 1893, at Chicago; also, BOREL et DRACH, Théorie des Nombres et Algèbre supérieure, 1895.

† GALOIS, "Sur la théorie des nombres," *Bulletin des Sciences mathématiques* de M. Férussac, 1830; reprinted in *Journal de mathématiques pures et appliquées*, 1846.

‡ Cours d'Algèbre supérieure, vol. 2, pp. 122–211.

§ Traité des Substitutions, § 21.

$$\xi^{p^{nl}} - \xi$$

if and only if l be a multiple of m.

4. Determination of the number N of $IQ[v, p^n]$. Let V denote the product of all such quantics. If v be a prime

$$V = \frac{\xi^{p^{nv}} - \xi}{\xi^{p^n} - \xi}, \qquad N = \frac{p^{nv} - p^n}{v},$$

If $v = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}$, $q_1, q_2, \cdots, q_m$ being different primes, the value of V is given as in Serret, l. c., p. 139, by taking instead of Serret's symbol

$$[\lambda] = \xi^{p^{n\lambda}} - \xi.$$

Hence we have

$$N = \frac{1}{v}\left(p^{nv} - \Sigma p^{\frac{nv}{q_1}} + \Sigma p^{\frac{nv}{q_1 q_2}} - \cdots + (-1)^m p^{\frac{nv}{q_1 q_2 \cdots q_m}}\right).$$

We find for N two simple limits:

$$\frac{p^{nv} - p^n}{v} < N < \frac{\varphi(v)}{v-1} \cdot \frac{p^{nv} - p^n}{v}.$$

5. A theoretic method due to Galois to decompose a quantic into its irreducible factors in the $GF[p^n]$ is to seek its greatest common divisor with successively $\xi^{p^n} - \xi$, $\xi^{p^{2n}} - \xi$, etc. Theoretically we can find all $IQ[v, p^n]$ by ridding $\xi^{p^{nv}} - \xi$ of all factors common with

$$\xi^{p^{n\mu}} - \xi \qquad (\mu = 1, 2, \cdots v - 1).$$

6. The expression for the product V of all $IQ[v, p^r]$ which belong to the exponent n, a *proper* divisor of $p^{rv} - 1$ (*i. e.*, n does not divide $p^{r\mu} - 1$ for $\mu < v$), is exactly that given in Serret, pp. 145–6. The number of such quantics is $\varphi(n)/v$.

7. If $F(\xi)$ be an $IQ[v, p^n]$ which belongs to the exponent $p^{nv} - 1$, then a root of $F(\xi) = 0$ is a *primitive* root of the $GF[p^{nv}]$. (Cf. Serret, §§ 353 and 369.)

8. If we have formed the N quantics $IQ\ [\mu, p^r]$ which belong to the exponent $(p^{r\mu} - 1)/d$ and if we replace ξ by ξ^λ, λ being prime to d and containing no prime factor other than those of $p^{r\mu} - 1$, we obtain *the* N quantics $IQ\ [\lambda\mu, p^r]$ which belong to the exponent $\lambda\,(p^{r\mu} - 1)/d$. In case p^r is of the form $4m - 1$ and μ is odd, λ must not be a multiple of 4.

9. Let $p^r = 2^i t - 1$, $i \geqq 2$, t odd; let $\lambda = 2^j s$, $j \geqq 2$, s odd; let k be the smaller of i and j. Let finally μ be odd.

If then we have formed the $N/2^{k-1}$ quantics $IQ\ [\mu, p^r]$ which belong to the exponent $(p^{r\mu} - 1)/d$ and we replace ξ by ξ^λ, λ being of the form indicated and prime to d and containing only the prime factors occurring in $p^{r\mu} - 1$, we obtain the $N/2^{k-1}$ quantics of degree $\lambda\mu$, each decomposing into 2^{k-1} quantics, so that we obtain N in all $IQ\left[\frac{\lambda\mu}{2^{k-1}}, p^r\right]$ belonging to the exponent $\lambda\,(p^{r\mu} - 1)/d$.

10. Let ρ be a primitive root in the $GF[p^r]$, λ an integer with no prime factor other than those of $p^r - 1$, e an integer prime to λ, d the greatest common divisor of e and $p^r - 1$.

(1) If $p^r = 4m + 1$ or 2^r, or if, when $p^r = 4m - 1$, λ is odd or the double of an odd number, $\xi^\lambda - \rho^e$ is an $IQ\ [\lambda, p^r]$ belonging to the exponent $\lambda\,(p^r - 1)/d$. We get thus every irreducible binomial in the $GF[p^r]$.

(2) If p^r, λ and k be defined as in § 9, $\xi^\lambda - \rho^e$ decomposes into 2^{k-1} $IQ\ [\lambda/2^{k-1}, p^r]$ belonging to the exponent $\lambda\,(p^r - 1)/d$.

11. Since irreducible binomials are lacking in the latter case, we proceed to set up trinomials $IQ\ [\lambda, p^r]$, for indeed every even integer λ which contains no other prime factors than those of $p^r - 1$. We have $p^r = 2^i t - 1$, t odd. Let $v = 2^{i-1}\lambda$. We may then determine two integers l and h such that

$$l \cdot 2^i - h\,(p^r - 1) = e + (p^r - 1)/2.$$

Then will

$$\xi^v - \rho^e = \xi^{\lambda \cdot 2^{i-1}} + \rho^{l \cdot 2^i}$$

decompose in the $GF[p^n]$ into the product

$$\prod_{m=1}^{2^{i-1}} (\xi^\lambda - \eta_m \rho^l \xi^{\lambda/2} - \rho^{2l}),$$

where η_m are the roots of $E(\eta) = 0$, $E(\eta)$ being the sum of the $2^{i-1} st$ powers of the roots of

$$X^2 - \eta X - 1 = 0.$$

But Waring's formula for the sum of the n^{th} powers of its roots gives, for $n =$ even*

* It is interesting to note that for n odd the quantic $S_n(\eta)$ represents a substitution on p^r letters, if only $p^{2r} - 1$ is relatively prime to n, *i. e.*, $S_n(\eta) = \beta$ has one and but one solution η in the $GF[p^r]$ for β an arbitrary mark of that field. Cf. L. E. DICKSON, "The analytic representation of substitutions," etc., *Annals of Mathematics*, 1897. Here we see that $S_n(\eta)$, for $n = 2^{i-1}$, completely decomposes in the $GF[p^r = 2^i t - 1]$.

$$S_n = n \sum_{s=0}^{n/2} \frac{(n-s-1)!}{s!\,(n-2s)!}\,\eta^{n-2s}$$

where we understand $n! = 1$ if $n = 0$. Hence

$$E(\eta) = \eta^{2^{i-1}} + 2^{i-1} \sum_{s=1}^{2^{i-2}-1} \frac{(2^{i-1}-s-1)!}{s!\,(2^{i-1}-2s)!}\,\eta^{2^{i-1}-2s} + 2.$$

As in Serret, p. 160–1, $E(\eta)$ is a factor (modulo p) of $\eta^{p^r-1} - 1$, *i. e.*, $E(\eta) = 0$ has 2^{i-1} roots in the $GF[p^r]$.

12. Theorem (Cf. Serret §§ 366 and 368): If $F(\xi)$ and $\varphi(\xi)$, of degrees v and μ (a divisor of v) respectively, belong to and are irreducible in the $GF[p^n]$, the equation

$$\varphi(\xi) = 0$$

has in the $GF[p^{nv}]$ exactly μ roots, viz:

$$X, X^{p^n}, X^{p^{2n}}, \cdots X^{p^{n(\mu-1)}}.$$

In particular $F(\xi)$ itself has the v roots

$$\xi, \xi^{p^n}, \cdots \xi^{p^{n(v-1)}}$$

a result due to Galois (for $n = 1$).

13. If $\Phi(\xi)$ belongs to the $GF[p^n]$ and is of degree m, we can find an $IQ[v, p^n]$ such that $\Phi(\xi) = 0$ has m roots in the $GF[p^{nv}]$.

14. Theorem (announced by Galois and proved by Serret for $n = 1$, §§ 370–1): Supposing known *one* $F(\xi)$ an $IQ[v, p^n]$ and by means of it a primitive root X of the $GF[p^{nv}]$ we can find *all* such quantics $\varphi(\xi)$ of degree v or a divisor of v; and thus we can completely decompose $\xi^{p^{nv}} - \xi$ in the $GF[p^n]$. Thus to obtain all of degree v which belong to an exponent t, a *proper* divisor of $p^{nv} - 1$, set the latter $= mt$ and take in turn for e each of the multiples of m which are prime to t. Then will

$$\varphi(\xi) = (\xi - X^e)(\xi - X^{ep^n}) \cdots (\xi - X^{ep^{n(v-1)}}).$$

Complete determination of the $IQ[p, p^n]$.*

15. To effect the decomposition of $\xi^{p^{np}} - \xi$ in the $GF[p^n]$, set

$$X_\mu = \xi^{p^{n\mu}} - \mu\xi^{p^{n(\mu-1)}} + \cdots + (-1)^k \cdot \frac{\mu(\mu-1)\cdots(\mu-k-1)}{1\cdot 2\cdots k}$$

* Cf. *Serret*, l.c., Section III, Chapter IV.

$$\xi^{p^{n(\mu-k)}} + \cdots + (-1)^{\mu}\xi.$$

Then $$X_{\mu+1} = X_{\mu}^{p^n} - X_{\mu},$$

$$X_p = X_1 (X_1^{p^n-1} - 1)\ (X_2^{p^n-1} - 1) \cdots (X_{p-1}^{p^n-1} - 1).$$

But $$X_1 = \xi^{p^n} - \xi,\ X_p = \xi^{p^{np}} - \xi.$$

Thus, if V denotes the product of all the quantics sought

$$V = \prod_{i=1}^{p-1} (X_i^{p^n-1} - 1).$$

But $$X_i^{p^n-1} - 1 = \prod_{j=1}^{p^n-1} (X_i - \nu_j),$$

ν_j running over all the marks ± 0 of the $GF[p^n]$.

According to the index i we distinguish $p-1$ *classes of* $IQ[p, p^n]$.

16. Consider first the factor

$$\xi^{p^n} - \xi - \nu$$

which is the product of p^{n-1} $IQ[p, p^n]$ of the first class.

Generalizing a decomposition or Mathieu *

$$\lambda(\xi^{p^n} - \xi - \nu) = \prod_{j=0}^{p^{n-1}-1} (\lambda^p \xi^p - \lambda\xi - \beta_j),$$

where β_j must be a root of

$$\eta^{p^{n-1}} + \eta^{p^{n-2}} + \cdots + \eta^p + \eta = \lambda\nu.$$

and hence also of

$$\eta^{p^n} - \eta = (\lambda\nu)^p - \lambda\nu.$$

If the decomposition shall take place in the $GF[p^n]$, λ and β_j must be marks of that field and hence $\lambda \cdot \nu$ must be an integer. Inversely β_j may be taken arbitrarily in the field, for the corresponding value for $\lambda \cdot \nu$ is an integer, the p^{th} power of

$$\beta^{p^{n-1}} + \cdots + \beta^p + \beta$$

being equal to itself.

In particular the quantic

Journal de mathématiques pures et appliquées, p. 280, 1861.

$$\xi^v - \xi - s \qquad (s = \text{integer} \not\equiv 0)$$

is irreducible in the $GF[p^n]$ if and only if

$$s^{p^{n-1}} + \cdots + s^p + s = ns \not\equiv 0,$$

i. e., if n is not a multiple of p (compare Serret's case, § 360).

17. Consider in particular

$$\xi^{p^n} - \xi - 1 = 0$$

and let I be a root of one of its irreducible factors,

$$\xi^v - \xi - \beta = 0,$$

so that we have

$$\beta + \beta^p + \cdots + \beta^{p^{n-1}} = 1.$$

Its other roots are $I+1, I+2, \cdots I+p-1$. Likewise the roots of

$$\lambda^p \xi^v - \lambda\xi - \beta = 0$$

are

$$I/\lambda, (I+1)/\lambda, \cdots (I+p-1)/\lambda.$$

Consider finally the irreducible equation

$$\xi^p - \xi - \delta = 0,$$

which belongs to the factor

$$\xi^{p^n} - \xi - (\delta + \delta^p + \cdots + \delta^{p^{n-1}}).$$

I say that it is satisfied by $(\delta + \delta^p + \cdots + \delta^{p^{n-1}})\, I + \alpha$, α being suitably chosen in the $GF[p^n]$. For the condition on α is

$$\alpha^p - \alpha - \tau = 0,$$

where

$$\tau = \delta - \beta(\delta + \delta^p + \cdots + \delta^{p^{n-1}}).$$

Then

$$\alpha^{p^n} - \alpha = \tau + \tau^p + \cdots + \tau^{p^{n-1}}$$

$$= (\delta + \delta^p + \cdots + \delta^{p^{n-1}})(1 - \beta - \beta^p - \cdots - \beta^{p^{n-1}}) = 0.$$

Hence all the roots of every $IQ[p, p^n]$ of the first class are linear functions of I.

18. THEOREM. *The irreducible quantics of class μ have as roots integral functions of I of degree μ.*

Let such a quantic have as root the function belonging to the $GF[p^n]$:

$$f(I) \equiv \sum_{j=0}^{p-1} a_j F. \tag{1}$$

Then will $f(I)$ be a root of $X_\mu = \sigma$, σ being a mark properly chosen. If we make this substitution, applying the identity

$$[f(I)]^{p^{nm}} = f(I^{p^{nm}}) = f(I + m),$$

which follows from $I^{p^n} = I + 1$, we find that

$$f(I+\mu) - \mu f(I+\mu-1) + \frac{\mu(\mu-1)}{1\cdot 2} f(I+\mu-2) \cdots + (-1)^\mu f(I) = \sigma.$$

The degree of this equation in I being $< p$, it is an identity. But the first member is the μ^{th} difference of $f(I)$ with respect to the constant difference 1 for I. Since it reduces to the constant $\sigma \neq 0$, the degree of $f(I)$ is exactly μ. Hence

$$a_\mu = \frac{\sigma}{\mu!}, \; a_{\mu+1} = a_{\mu+2} = \cdots = a_{p-1} = 0.$$

19. General expression for all $IQ[p, p^n]$.

Suppose the quantic $f(I)$ given by (1) does not reduce to a_0; but otherwise the a_j's are supposed arbitrary. Form the equations

$$I^\lambda [f(I) - \xi] = 0 \qquad (\lambda = 0 \cdots p-1) \tag{2}$$

We may lower the exponents below p by using

$$I^p = I + \beta.$$

The general one of the equations (2) then becomes

$$\beta a_{p-\lambda} + (\beta a_{p-\lambda+1} + a_{p-\lambda}) I + (\beta a_{p-\lambda+2} + a_{p-\lambda+1}) I^2 + \cdots + (\beta a_{p-1} + a_{p-2}) I^{\lambda-1} + (a_0 + a_{p-1} - \xi) I^\lambda + a_1 I^{\lambda+1} + a_2 I^{\lambda+2} + \cdots + a_{p-1-\lambda} I^{p-1} = 0.$$

Eliminating the powers $I^0, I^1, \cdots I^{p-1}$ between these p equations, we reach the irreducible quantic in ξ:

$$\begin{vmatrix} a_0-\xi & a_1 & a_2 & \cdots a_{p-2} & a_{p-1} \\ \beta a_{p-1} & a_0+a_{p-1}-\xi & a_1 & \cdots a_{p-3} & a_{p-2} \\ \beta a_{p-2} & \beta a_{p-1}+a_{p-2} & a_0+a_{p-1}-\xi & \cdots a_{p-4} & a_{p-3} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \beta a_2 & \beta a_3+a_2 & \beta a_4+a_3 & \cdots a_0+a_{p-1}-\xi & a_1 \\ \beta a_1 & \beta a_2+a_1 & \beta a_3+a_2 & \cdots \beta a_{p-1}+a_{p-2} & a_0+a_{p-1}-\xi \end{vmatrix}$$

which gives the most general $IQ[p, p^n]$.

To obtain those of class μ set $a_{\mu+1} = a_{\mu+2} = \cdots = a_{p-1} = 0$. Giving to $a_0, a_1, \cdots a_{\mu-1}$ all possible values in the $GF[p^n]$ and to a_μ every value $\neq 0$, we obtain $p^{n\mu}(p^n - 1)$ quantics. But if we had started with another root $f(I + m)$ of the above determinant, m being an integer, in place of $f(I)$, we would have reached the same quantic. Hence there are exactly $p^{n\mu-1}(p^n - 1)$ $IQ[p, p^n]$ of class μ, as we also readily see from § 15.

For $\mu = 1$, we find the $IQ[p, p^n]$:

$$\xi^p - a_1^{p-1}\xi - (a_0^p - a_0 a_1^{p-1} + \beta a_1^p).$$

20. An interesting type of $IQ[p, p^n]$ of class $p - 1$ is given by setting every a_j equal zero except a_0 and a_{p-1}, viz.:

$$F(\xi) \equiv (\xi - a_0 - a_{p-1})^p + a_{p-1}(\xi - a_0 - a_{p-1})^{p-1} - \beta^{p-1} a_{p-1}^p.$$

Multiplying by $\xi - a_0 - a_{p-1}$, we have

$$\xi^p = \frac{\xi[a_0^p + a_{p-1}^p(\beta^{p-1}+1)] - [a_0^{p+1} + \beta^{p-1}a_{p-1}^{p+1} + a_0 a_{p-1}^p(\beta^{p-1}+1)]}{\xi - a_0}$$

But the roots of $F(\xi) = 0$ can be represented thus

$$\xi,\ \xi^{v^n},\ \xi^{v^{2n}},\ \cdots \xi^{v^{n(p-1)}}.$$

Hence its roots may all be expressed as linear fractional functions of one of them.

21. We may prove as in Serret, §§ 381–2, that the product of all $IQ[p^s, p^n]$ is given by

$$\prod_{m=p^{s-1}}^{p^s-1} (X_m^{p^n-1} - 1)$$

Of these $p^s - p^{s-1}$ factors, the λ^{th} is said to be the product of the $IQ[p^s, p^n]$ of *class* λ. For $\lambda = p^s - p^{s-1}$ we have the *principal* class.

THEOREM. If $F(\xi)$ be an $IQ[p^s, p^n]$ belonging to the class λ (not the principal), $F(\xi^{p^n} - \xi)$ decomposes into p^n $IQ[p^s, p^n]$ of the class $\lambda + 1$; but if the former belong to the principal class, the latter is simply an $IQ[p^{s+1}, p^n]$ of the first class.

PARIS, *April* 15, 1897.

ON A SOLUTION OF THE BIQUADRATIC WHICH COMBINES THE METHODS OF DESCARTES AND EULER.

BY DR. EMORY McCLINTOCK.

[Read at the May meeting of the Society, 1897.]

THE product of

$$x^2 - v^{\frac{1}{2}} x + \tfrac{1}{2}(p + v + qv^{-\frac{1}{2}}) = 0 \qquad (1)$$

and

$$x^2 + v^{\frac{1}{2}} x + \tfrac{1}{2}(p + v - qv^{-\frac{1}{2}}) = 0 \qquad (2)$$

is

$$x^4 + px^2 + qx + \tfrac{1}{4}[(p+v)^2 - q^2v^{-1}] = 0. \qquad (3)$$

All of this except one term coincides with the short form of the general biquadratic,

$$x^4 + px^2 + qx + r = 0. \qquad (4)$$

Since v is at our disposal we may treat (3) and (4) as equivalent, term by term, so that we have, after clearing ing of fractions,

$$4rv = v(p + v^2) - q^2,$$

$$v^3 + 2pv^2 + (p^2 - 4r)v - q^2 = 0.* \qquad (5)$$

* Up to this point this solution is precisely that of Descartes, except that the indeterminate quantity is here introduced in the form of a square root. It seems remarkable that the extreme facility with which the method of Descartes, which consists in separating the biquadratic into quadratic factors, may be combined with that of Euler, which consists in exhibiting the roots of the biquadratic as sums of square roots of the three roots of a cubic, should not heretofore have been observed. If the combination should, contrary to the writer's expectation, be found lacking in novelty, it may nevertheless be held that it has not attracted the attention which it deserves.