highest value of r for which the congruence $\lambda^r\omega \equiv 0$, (mod p^r), is satisfied.

When p is a prime of the second category, so that $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, the criteria for the divisibility of $x+y\theta+z\theta^2$ by $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, respectively, may be written

$$\left.\begin{aligned} x-a_1y-b_1z &\equiv 0, \\ x-a_2y-b_2z &\equiv 0, \\ x-a_3y-b_3z &\equiv 0, \end{aligned}\right\} \quad (\text{mod } p),$$

and as a verification it may be observed that if all these conditions are satisfied, it follows that

$$x \equiv y \equiv z \equiv 0, \quad (\text{mod } p),$$

that is, $x+y\theta+z\theta^2$ is divisible by p.

Finally, if p is a prime of the third category, $x+y\theta+z\theta^2$ is divisible by p only if

$$x \equiv y \equiv z \equiv 0, \quad (\text{mod } p).$$

These congruential relations are analogous to those employed by Kummer in his papers on ideal primes.

On the Algebraical Integers derived from an Irreducible Cubic Equation. By G. B. Mathews. Received May 29th, 1893. Read June 8th, 1893.

1. Let θ, θ', θ'' be the roots of the irreducible cubic

$$f(\theta) = \theta^3+\alpha\theta^2+\beta\theta+\gamma = 0,$$

where α, β, γ are ordinary integers. Then there will be associated with it three conjugate *corpora* $\Omega(\theta)$, $\Omega(\theta')$, $\Omega(\theta'')$, the corpus $\Omega(\theta)$ being made up of the aggregate of all quantities such as

$$\omega = \frac{x+y\theta+z\theta^2}{t},$$

x, y, z, t being ordinary integers; and similarly for $\Omega(\theta')$, $\Omega(\theta'')$. (The conjugate corpora may or may not be distinct.)

In order that ω may be an algebraical integer it is necessary and sufficient that, ω', ω'' being conjugate to ω, the quantities

$$\omega+\omega'+\omega'', \quad \omega'\omega''+\omega''\omega+\omega\omega', \quad \omega\omega'\omega''$$

shall be rational integers; and this leads to three congruences which must be satisfied by x, y, z, namely,

$$3x-\alpha y+(\alpha^2-2\beta)\,z\equiv 0, \ (\text{mod } t)\ \ldots\ldots\ldots\ldots\ldots\ldots(1),$$

$$3x^2+\beta y^2+(\beta^2-2\gamma\alpha)\,z^2-(\alpha\beta-3\gamma)yz+2(\alpha^2-2\beta)zx-2\alpha xy\equiv 0, \ (\text{mod } t^2) \ \ldots\ldots\ldots\ldots\ldots(2),$$

$$x^3+\gamma y^3+\gamma^2z^3-\alpha x^2y+(\alpha^2-2\beta)\,x^2z+\beta xy^2+(\beta^2-2\gamma\alpha)\,xz^2-(\alpha\beta-3\gamma)\,xyz$$
$$+\alpha\gamma y^2z+\beta\gamma yz^2\equiv 0, \ \ (\text{mod } t^3)\ \ldots\ldots\ldots\ldots\ldots\ldots(3).$$

2. It will be supposed, in the first instance, that t is prime to 3. Then the second and third congruences are not affected if they are multiplied by 3 and 27 respectively, and the moduli left unaltered; x may then be eliminated by putting

$$3x=\xi t+\alpha y-(\alpha^2-2\beta)\,z.$$

In order to express the results in the most convenient form, the following abbreviations will be used:—

$$\left.\begin{aligned} u &= y-\alpha z\\ A &= 3\beta-\alpha^2, \quad B=9\gamma-\alpha\beta, \quad C=3\alpha\gamma-\beta^2\\ P &= 2\alpha^3-9\alpha\beta+27\gamma, \quad Q=\alpha^2\beta+9\alpha\gamma-6\beta^2\\ R &= 6\alpha^2\gamma-\alpha\beta^2-9\beta\gamma, \quad S=9\alpha\beta\gamma-2\beta^3-27\gamma^2\\ D &= \tfrac{1}{3}(B^2-4AC)=27\gamma^2+4\beta^3+4\alpha^3\gamma-\alpha^2\beta^2-18\alpha\beta\gamma \end{aligned}\right\}\ldots\ldots(4).$$

D may be called the discriminant of $f(\theta)$, and it will be observed that $(A, B, C \between \theta, 1)^2$ is the Hessian, and $(P, Q, R, S \between \theta, 1)^3$ the cubicovariant of $f(\theta)$, each with its coefficients absolutely determined.

The congruence (1) may now be written

$$3x-\alpha u-2\beta z\equiv 0, \quad (\text{mod } t)\ \ldots\ldots\ldots\ldots\ldots\ldots(5),$$

and if we substitute $\alpha u+2\beta z+\xi t$ for $3x$ in (2), after multiplying by 3, it will be found that the term in t on the left hand vanishes identically, and that (2) is replaced by the equivalent congruence

$$Au^2+Buz+Cz^2\equiv 0, \quad (\text{mod } t^2)\ldots\ldots\ldots\ldots\ldots(6).$$

When the same substitution is made in (3), after multiplying by 27, the coefficient of t^2 vanishes identically; the coefficient of t may be reduced to the form $3\xi t\,(Au^2+Buz+Cz^2)$, which, on account of the congruence last written, is a multiple of t^3, and may therefore be omitted; and finally, after some algebraical reductions, it is found that (3) may be replaced by

$$Pu^3+3Qu^2z+3Ruz^2+Sz^3 \equiv 0, \quad (\text{mod } t^3) \ldots\ldots\ldots\ldots(7).$$

3. It is now necessary to discuss the simultaneous congruences (6) and (7). Unfortunately, this is a matter of considerable difficulty, because the algebraical theory of elimination cannot be applied except under certain limitations. By following the analogy of Sylvester's dialytic method of elimination, we may establish the theorem that, if R is the algebraical resultant of two binary quantics $F(x, y)$, $G(x, y)$, then, in order that the simultaneous congruences

$$F(x, y) \equiv 0, \quad G(x, y) \equiv 0, \quad (\text{mod } m),$$

may admit of solutions such that no common factor of x and y may divide m, it is *necessary* that $R \equiv 0$, (mod m).

Now in the congruences (6) and (7), we may suppose that u and z have no common factor which divides t; for, if they had, it would follow from (5) and (4) that x, y, z, t would all have a common factor, and hence $(x+y\theta+z\theta^2)/t$ would not be in its lowest terms. Therefore supposing, as we may do, that ω is in its lowest terms, and observing that the resultant of $(A, B, C \between u, z)^2$ and $(P, Q\, R, S \between u, z)^3$ is $27D^3$, we infer from (6) and (7) that

$$27D^3 \equiv 0, \quad (\text{mod } t^2)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(8).$$

If t is not prime to 3, we must write instead of (6) and (7),

$$Au^2+Buz+Cz^2 \equiv 0, \quad (\text{mod } 3t^2) \ \ldots\ldots\ldots\ldots(9),$$

$$Pu^3+3Qu^2z+3Ruz^2+Sz^3 \equiv 0, \quad (\text{mod } 27t^3)\ldots\ldots(10),$$

and consequently, instead of (8),

$$27D^3 \equiv 0, \quad (\text{mod } 3t^2).$$

Both cases are included in

$$9D^3 \equiv 0, \quad (\text{mod } t^2) \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots(11),$$

and the conclusion is that the investigation may be confined to those integers t the squares of which divide $9D^3$.

4. There are so many different cases to consider, according to the distribution of the prime factors of A, B, C, P, Q, R, S, and D, that it seems best not to attempt a complete enumeration. The congruences (6) and (7) or (9) and (10) must, of course, be fully discussed in any particular case that may arise; there is no difficulty in doing this when the function $f(\theta)$ has once been chosen.

There are one or two specially interesting cases which deserve attention, and will serve to illustrate the theory.

The first of these is when the congruences (6) and (7) are satisfied *identically*; that is to say, when

$$A \equiv B \equiv C \equiv 0, \quad (\text{mod } t^2) \ldots\ldots\ldots\ldots\ldots (12),$$

$$P \equiv Q \equiv R \equiv S \equiv 0, \quad (\text{mod } t^3).$$

These are equivalent to two distinct conditions, which may be expressed by

$$A \equiv 0, \quad (\text{mod } t^2),$$

$$P \equiv 0, \quad (\text{mod } t^3) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (13);$$

and it will be found that D is divisible by t^6. The integers u and z may be chosen at pleasure, and then $y = u + \alpha z$, and x, y, z are connected by the single relation

$$3x - \alpha y + (\alpha^2 - 2\beta) z \equiv 0, \quad (\text{mod } t);$$

or, say,
$$x \equiv \lambda y + \mu z, \quad (\text{mod } t) \ldots\ldots\ldots\ldots\ldots\ldots (14),$$

where λ, μ are determinate to modulus t. Suppose they have their least positive values, then the general form of ω for this value of t is

$$\omega = \frac{(\lambda + \theta) y + (\mu + \theta^2) z}{t} + hy + kz,$$

where h, k are rational integers. The essentially new integers thus introduced are

$$\omega_1 = \frac{\lambda + \theta}{t}, \quad \omega_2 = \frac{\mu + \theta^2}{t};$$

and it may be observed that, since

$$\theta = t\omega_1 - \lambda, \quad \theta^2 = t\omega_2 - \mu,$$

the modulus $[1, \omega_1, \omega_2]$ includes all the elements of the modulus $[1, \theta, \theta^2]$, and besides these a portion of the remaining integers in $\Omega(\theta)$.

In order to construct a case of this kind, suppose $a = 1$, $t = 5$; then the congruences $A \equiv 0$, (mod 25), $P \equiv 0$, (mod 125), give

$$3\beta-1 \equiv 0, \quad (\text{mod } 25),$$

$$27\gamma-9\beta+2 \equiv 0, \quad (\text{mod } 125).$$

If we take $\beta = 17$, the first congruence is satisfied, and the second leads to $\gamma \equiv 38$, (mod 125). It will be found that $\gamma = 38$ leads to a reducible equation in θ; but if we take $\gamma = 163$, we have the irreducible equation

$$\theta^3+\theta^2+17\theta+163 = 0,$$

for which $A = 2.5^2$, $B = 58.5^2$, $C = 8.5^2$,

$$P = 34.5^3, \quad Q = -2.5^3, \quad R = -194.5^3, \quad S = -5618.5^3,$$

$$D = 11.2^2.5^6.$$

The congruence (5) reduces to

$$x \equiv 2y+z, \quad (\text{mod } 5),$$

so that

$$\omega = \frac{(2+\theta)\,y+(1+\theta^2)\,z}{5}$$

is an integer when y, z are rational integers; and, as a verification, it will be found that if we put

$$\omega_1 = \frac{2+\theta}{5}, \quad \omega_2 = \frac{1+\theta^2}{5},$$

these quantities satisfy the equations

$$\omega_1^3-\omega_1^2+\omega_1+1 = 0,$$

$$\omega_2^3+6\omega_2^2-4\omega_2-212 = 0.$$

It is noticeable that ω_1 is an algebraical unit; and also that ω_2 is an integral function of ω_1, because

$$5\omega_2-1 = (5\omega_1-2)^2,$$

and hence

$$\omega_2 = 5\omega_1^2-4\omega_1+1.$$

5. The latter circumstance is not accidental; for if, as above, we put

$$\omega_1 = \frac{\lambda+\theta}{t}, \quad \omega_2 = \frac{\mu+\theta^2}{t},$$

we have
$$(t\omega_1-\lambda)^2 = t\omega_2-\mu,$$
and
$$\omega_2 = t\omega_1^2-2\lambda\omega_1+\frac{\lambda^2+\mu}{t};$$
now
$$3\lambda \equiv \alpha, \pmod{t},$$
$$3\mu \equiv -\alpha^2+2\beta;$$
and therefore
$$9(\lambda^2+\mu) \equiv (6\beta-2\alpha^2)$$
$$\equiv 2A \equiv 0, \pmod{t};$$

that is, $(\lambda^2+\mu)/t$ is an integer, and ω_2 is an integral function of ω_1. Hence it may be inferred that the corpora $\Omega(\theta)$ and $\Omega(\omega_1)$ are identical in content; but the discriminant of $\Omega(\omega_1)$ is D/t^6 instead of D.

Thus, for the equation
$$\theta^3-\theta^2+\theta+1 = 0 \quad \text{..........................(15)}$$
(where θ has been written instead of ω_1),
$$A = 2, \quad B = 10, \quad C = -4,$$
$$D = 44.$$

Since D is divisible by the square of 2, we might expect to find integers of the form $(x+y\theta+z\theta^2)/2$; however, such integers do not exist, for the auxiliary congruences (6), (7) in this case are, on reduction,
$$u^2+uz \equiv 0, \pmod{2},$$
$$u^3-u^2z+uz^2+z^3 \equiv 0, \pmod{4},$$
and these can only be satisfied simultaneously if $u \equiv z \equiv 0$, (mod 2), leading to $x \equiv y \equiv z \equiv 0$, (mod 2).

It may be proved without difficulty that there are no integers of the form $(x+y\theta+z\theta^2)/11$, and hence that the equation (15) defines what may be called a primitive corpus $\Omega(\theta)$, that is, one which contains no integers except those of the form $x+y\theta+z\theta^2$ with x, y, z integral.

It may be worth while to observe that, since
$$4(Ax^2+Bx+C)^3+(Px^3+3Qx^2+3Rx+S)^2$$
$$= 27D(x^3+\alpha x^2+\beta x+\gamma)^2 \text{.........(16)}$$

identically, it follows that, whenever A, B, C are divisible by t^3, and D is divisible by t^6,

$$Px^3+3Qx^2+3Rx+S \equiv 0, \quad (\text{mod } t^3),$$

identically; so that it is unnecessary to calculate the values of P, Q, R, S.

6. Another interesting case is when the congruence (6) is satisfied identically, but not (7). It follows from the identities

$$P = -2aA+3B, \quad Q = -2\beta A+aB,$$
$$R = -\beta B+2aC, \quad S = -3\gamma B+2\beta C,$$

that P, Q, R, S are all divisible by t^2, but not by t^3. Now multiply (7) by P^2, and change the modulus to t^7; then the new congruence, equivalent to the old one, is

$$(Pu+Qz)^3-3\,(Q^2-PR)(Pu+Qz)\,z^2$$
$$+(P^2S-3PQR+2Q^3)\,z^3 \equiv 0, \quad (\text{mod } t^7).$$

But Q^2-PR is a multiple of DA, and therefore of t^6; hence the second term is divisible by t^8. Also $P^2S-3PQR+2Q^3$ is divisible by D^2, and therefore by t^8, so that the congruence reduces to

$$(Pu+Qz)^3 \equiv 0, \quad (\text{mod } t^7),$$

whence
$$\left(\frac{P}{t^2}u+\frac{Q}{t^2}z\right)^3 \equiv 0, \quad (\text{mod } t);$$

and, if t is not divisible by any cube, this leads to

$$Pu+Qz \equiv 0, \quad (\text{mod } t^3).$$

[If t is divisible by a cube, some modification is necessary; but, as already said, it seems best to omit these discussions of detail.]

The solution of this congruence will be of the form

$$u \equiv kz, \quad (\text{mod } t),$$

where k is determinate to modulus t; and therefore it will follow that

$$y \equiv qz, \quad x \equiv pz, \quad (\text{mod } t),$$

where p, q may be taken to be determinate numbers between 0 and t; so that, instead of obtaining, as in the last case, *two* integers ω_1 and ω_2 (or ω_1 and ω_1^2), of which the form is fractional, we shall have only one, namely,

$$\omega_1 = \frac{p+q\theta+\theta^2}{t}.$$

Of the conditions
$$A = 3\beta - \alpha^2 \equiv 0, \pmod{t^2},$$
$$B = 9\gamma - \alpha\beta \equiv 0,$$
$$C = 3\alpha\gamma - \beta^2 \equiv 0,$$
only two are independent, because
$$\beta A - \alpha B + 3C = 0$$
identically, so that if $A \equiv 0$ and $B \equiv 0$, it follows that $C \equiv 0$, always supposing that t is prime to 3.

If t and α are assigned, suitable values of β and γ may be found from
$$3\beta \equiv \alpha^2, \pmod{t^2}, \quad 27\gamma \equiv \alpha^3, \pmod{t^2}.$$

For instance, if $\alpha = 1$, $t = 5$, it will be found that $\beta \equiv 17$, $\gamma \equiv 13$, (mod 25); and, if we take θ to be a root of
$$\theta^3 + \theta^2 + 17\theta + 13 = 0,$$
which is irreducible,
$$A = 50, \quad B = 100, \quad C = -250, \quad D = 32.5^4,$$
$$P = 8.25, \quad Q = -64.25, \quad R = -88.25, \quad S = -496.25;$$
and the congruence (7) is
$$8(u^3 - 24u^2z - 33uz^2 - 62z^3) \equiv 0, \pmod{5},$$
that is,
$$8(u - 3z)^3 \equiv 0, \pmod{5};$$
therefore
$$u \equiv 3z, \quad y \equiv 4z, \quad x \equiv 4z, \pmod{5},$$
and all the integers of the set here considered are rational multiples of
$$\omega_1 = \frac{4 + 4\theta + \theta^2}{5}.$$

It will be found that ω_1 satisfies the equation
$$\omega_1^3 + 5\omega_1^2 + 15\omega_1 - 5 = 0.$$

The relation between θ and ω_1 may be expressed in the forms
$$\left.\begin{aligned} \omega_1^2 &= -3 - 4\theta, \\ 5\omega_1 &= 4 + 4\theta + \theta^2, \end{aligned}\right\} \qquad \left.\begin{aligned} \theta^2 &= \omega_1^2 + 5\omega_1 - 7, \\ 4\theta &= -\omega_1^2 - 3. \end{aligned}\right\}$$

For the equation satisfied by ω_1, we have
$$A = 20, \quad B = -120, \quad C = -300, \quad D = 2^9.5^2;$$

and, since A, B, C are divisible by 2^2, and D by 2^6, we shall have integers of the form

$$\eta = \frac{x+y\omega_1+z\omega_1^2}{2}.$$

Proceeding as already explained, it will be found that

$$\eta_1 = \frac{1+\omega_1}{2}, \quad \eta_2 = \frac{1+\omega_1^2}{2}$$

are integers; that $\quad \eta_2 = 2\eta_1^2-2\eta_1+1$;

and that η_1 is a root of the equation

$$\eta^3+\eta^2+2\eta-2 = 0,$$

for which $\quad A = 5, \quad B = -20, \quad C = -10,$

$$D = 200 = 2^3 . 5^2;$$

$$P = -70, \quad Q = -40, \quad R = 20, \quad S = -160.$$

On examining the auxiliary congruences (6) and (7) for $t = 2, 3, 5$, respectively, it will be found that they do not admit of solutions distinct from $u \equiv z \equiv 0$; hence $\Omega(\eta)$ is a primitive corpus.

It will be found that, writing η for η_1,

$$\omega_1 = 2\eta-1,$$

$$\theta = -\eta^2+\eta-1;$$

and these may be regarded as Tchirnhausen transformations by which the equations in ω_1 and θ may be derived from the equation in η. It may, I think, be inferred that every corpus that is not primitive may be derived from a primitive corpus by a transformation of this kind.

7. There is one other special case of the general theory which is of some practical importance. It may happen that D is divisible by t^2, while A and P are prime to t. In this case the congruences (6) and (7) are satisfied by putting

$$2Au+Bz \equiv 0, \quad (\text{mod } t),$$

$$Pu+Qz \equiv 0, \quad (\text{mod } t),$$

which are consistent, because

$$2AQ-BP = -9D \equiv 0, \quad (\text{mod } t^2).$$

(It is supposed that t is odd and prime to 3.)

As an example of this case, take

$$\theta^3+55\theta^2+67\theta+77=0,$$

which occurs in connexion with complex multiplication of elliptic functions for $\Delta=53$ (*Proc. Lond. Math. Soc.*, Vol. XXI., p. 217).

Here $$A=-8\,.\,353,\quad B=-8\,.\,374,\quad C=8\,.\,1027,$$
$$D=2^{10}\,.\,5^4\,.\,53,$$

while P is prime to 5. Hence, putting $t=25$, we find, after some reductions, that the auxiliary congruences give

$$x\equiv 13z,\quad y\equiv z,\quad (\text{mod } 25),$$

and the quantity $$\eta=\frac{13+\theta+\theta^2}{25}$$

satisfies the equation $\eta^3-115\eta^2+107\eta-25=0$.

For this equation

$$A=-8\,.\,1613,\quad B=8\,.\,1510,\quad C=-8\,.\,353,$$
$$D=2^{10}\,.\,53.$$

Now A, B, C are all divisible by 2^3, and D is divisible by 2^6; hence we find that

$$\omega=\frac{x+y\eta+z\eta^2}{2}$$

is integral if $$x\equiv y+z,\quad (\text{mod } 2).$$

Putting, then, $$\zeta=\frac{1+\eta}{2},$$

we find that $$\zeta^3-59\zeta^2+85\zeta-31=0,$$

an equation with

$$A=-2\,.\,1613,\quad B=4\,.\,1184,\quad C=-2\,.\,869,$$
$$D=2^4\,.\,53.$$

It will be found on trial that the corpus $\Omega\,(\zeta)$ is primitive, and that

$$\eta=2\zeta-1,$$
$$\theta=4\zeta^2-234\zeta+169.$$