TERNARY CHARACTERISTICS OF PRIMES*

BY E. T. BELL

1. *Introduction.* As will be seen from the proofs, the curious properties of primes given by the theorems of §2 are less abstruse than they seem at first sight. That they are obvious when once the clue to their derivation is given does not, however, detract from their interest.

Let μ be either of 1, 2, and λ a definite one of 0, 1. We shall denote the equation

$$x^2 - a[\lambda + (1 - \lambda)p^\alpha]y^2 - bq^\beta z^2 = \mu^2 \tag{1}$$

by its *characteristic* $[a, b, \lambda]$. Thus $[a, b, 0]$ is

$$x^2 - ap^\alpha y^2 - bq^\beta z^2 = \mu^2, \tag{2}$$

and $[a, b, 1]$ is

$$x^2 - ay^2 - bq^\beta z^2 = \mu^2. \tag{3}$$

To avoid separate statements, we do not distinguish the cases $[a, b, \lambda]$, $\lambda = 0, 1$, until necessary. In (1), $p, q, \alpha, \beta, x, y, z$ are variable integers subject only to the following restrictions: p, q are primes >2; $\alpha > 0$, $\beta > 0$ are $\equiv 1 \pmod 4$; $x > 0$, $y > 0$, $z > 0$; a, b are constant integers >0. If, subject to all these restrictions,

$$p = p', \quad q = q', \quad \alpha = \alpha', \quad \beta = \beta', \quad x = x', \quad y = y', \quad z = z'$$

is a set of values of $p, q, \alpha, \beta, x, y, z$ for which (1) is true, we shall call the matrix $(p', q', \alpha', \beta', x', y', z')$ a *solution* of (1). Note in particular that the definitions imply that p', q' in each solution are primes >2. The equation $[a, b, \lambda]$ is transcendental; α, β are variables. When $\lambda = 1$ we may omit p, α, p', α' from the definitions, since their retention is then trivial; a solution of $[a, b, 1]$ may be written $(*, q', *, \beta',$

*Presented to the Society, San Francisco Section, April 7, 1928.

x', y', z'). Solutions being matrices, their equality is defined. Unequal solutions will be called *distinct*.

If p', q' in a given solution are such that, for m constant and >2,

$$p' \equiv p_0', \quad q' \equiv q_0', \quad \bmod m, \quad p_0' > 0, \quad q_0' > 0,$$

we shall say that the solution has the *residue* $(p_0', q_0')_m$ *modulo* m.

A set consisting of an infinity of distinct solutions is said to be *infinite*. Infinite sets are called *distinct* when each of the sets contains an infinity of solutions not in any of the others.

An integer $D>0$ which determines the constants a, b, and λ, so that (1) has an infinite set of solutions will be called a *determinant* of $[a, b, \lambda]$. The precise way in which D determines $[a, b, \lambda]$ so as to have the stated property is immaterial for the moment.

Let c, n, r_j, s be constant integers, $c>0$, $n>2$, $r_j>0$ $(j=1, \cdots, s)$. Let the δ_j $(j=1, \cdots, s)$ be distinct primes >2 such that δ_j is prime to $c (j=1, \cdots, s)$ and

$$\delta_j \equiv r_j, \bmod n, \qquad (j = 1, \cdots, s);$$

and let the c_j be integers >0. Then, if every integer D of the form $c\delta_1^{c_1} \delta_2^{c_2} \cdots \delta_s^{c_s}$ is a determinant of $[a, b, \lambda]$, and if further the infinite sets of solutions appertaining to each pair of unequal determinants of this form are distinct, we shall call the set of all integers of the prescribed form a *discriminant* of $[a, b, \lambda]$, and write this discriminant $\{c, r_1^{c_1}, r_2^{c_2}, \cdots, r_s^{c_s}\}_n$.

Our object is to find discriminants, to exhibit a characteristic $[a, b, \lambda]$ for a given discriminant, to assign the residues of the solutions in each case, and to classify the solutions.

The solutions in certain infinite sets will be classified by separation in finite odd numbers of distinct infinite sets, called *periods*, such that all the solutions in a given period are derivable from a fundamental one, called the *source* of the period. These periods depend upon the following sequences

of integers; in the periods the integers in the sequences are all >0.

Let g, h denote constant integers both different from zero. Then (g, h) is called the *parameter* of the infinity of sequences $w_n (n=0, 1, \cdots)$ of integers defined by

$$w_{n+2} = gw_{n+1} - hw_n$$

and a pair (w_0, w_1) of initial integers. The particular pair of these sequences determined by the pairs of initial values

$$(w_0, w_1) = (0, 1), \quad (w_0, w_1) = (2, g)$$

are the *Lucas sequences* u_n, $v_n (n=0, 1, \cdots)$ respectively, for the parameter (g, h). All the periods in a given infinite set pertain to the same parameter (g, h); different determinants in a given discriminant give periods pertaining to different parameters. As the periods depend upon u_n, v_n, the numerous known properties of Lucas sequences can be applied to read off properties of solutions of $[a, b, \lambda]$. For convenience we add references concerning u_n, v_n.*

2. *Existence Theorems.* Among many others we can state the following three general theorems. These give considerable information regarding the situation described in §1.

There exist discriminants Δ such that, if D is a determinant in Δ, the following statements hold.

THEOREM I. *In addition to determining the characteristic* $[a, b, \lambda]$, *each* D *determines a unique matrix* (T, U) *of integers* $T>0$, $U>0$, *and an odd number* ω *of distinct matrices*

$$(p_j, q_j, \alpha_j, \beta_j, V_j, W_j), \quad (j = 1, \cdots, \omega),$$

in which V_j, W_j *are integers* >0, *such that*

$$\sigma_{jn} \equiv (p_j, q_j, \alpha_j, \beta_j, Uu_n, \mu V_j v_n/2, \mu W_j v_n/2),$$

$$(j = 1, \cdots, \omega; \quad n = 1, 2, \cdots),$$

* Lucas, American Journal of Mathematics, vol. 1, pp. 184, 289; *Théorie des Nombres*, Chapter 18; Bachmann, *Niedere Zahlentheorie*, Kap. 2; Dickson, *History of the Theory of Numbers*, vol. 1, Chapter 17.

are ω distinct infinite sets of solutions of $[a, b, \lambda]$; the u_n, $v_n (n=0, 1, \cdots)$ are the Lucas sequences for the parameter $(2T/\mu, 1)$. The infinite set σ_{jn} $(n=1, 2, \cdots)$ is a period (as described in §1) with the source

$$\sigma_{j1} = (p_j, q_j, \alpha_j, \beta_j, U, TV_j, TW_j),$$

the solution σ_{jn} being obtained from σ_{j1} by multiplying U, TV_j, TW_j by u_n, v_n/v_1, v_n/v_1 respectively. If $\lambda=1$, there is one and only one (q_j, β_j) for each (V_j, W_j).

THEOREM II. *The D as in Theorem* I *also determines a modulus m such that all the solutions $\sigma_{jn} (j=1, \cdots, \omega;\ n=1, 2, \cdots)$ have the same residue modulo m, and this residue remains constant as D ranges over all determinants in Δ.*

THEOREM III. *The matrices (T, U), and hence also the periods described in Theorem* I, *are distinct for unequal determinants D in Δ.*

3. *Specific Theorems for $\lambda=s=c_1=1$.* The relevant parameters to be assigned are c, r, n, which determine Δ, since $s=1$; a, b, which fix $[a, b, \lambda]$ when $\lambda=1$, and m, q_0', which

n, r, c	a, b	m, q_0'	n, r, c	a, b	m, q_0'
(1) 4, 1, 2	1, 1	8, 1	(19) 24, 11, 1	1, 1	12, 7
(2) 8, 1, 1	4, 1	8, 5	(20) 24, 11, 1	1, 2	12, 5
(3) 8, 3, 2	1, 1	8, 5	(21) 24, 13, 1	6, 1	24, 7
(4) 8, 3, 3	4, 1	8, 5	(22) 24, 17, 5	2, 1	24, 11
(5) 8, 3, 4	1, 1	8, 3	(23) 24, 17, 5	18, 1	24, 19
(6) 8, 5, 1	2, 1	8, 3	(24) 24, 19, 1	9, 2	12, 5
(7) 8, 5, 4	1, 1	8, 3	(25) 40, 7, 5	1, 2	20, 13
(8) 12, 5, 4	1, 1	24, 19	(26) 40, 7, 5	1, 2	20, 17
(9) 12, 5, 4	9, 1	24, 11	(27) 40, 11, 1	5, 2	20, 3
(10) 16, 3, 1	8, 1	8, 5	(28) 40, 11, 1	5, 2	20, 7
(11) 16, 7, 1	1, 2	8, 3	(29) 40, 19, 1	5, 2	20, 3
(12) 16, 7, 1	2, 1	8, 5	(30) 40, 19, 1	5, 2	20, 7
(13) 16, 7, 1	4, 1	8, 3	(31) 40, 23, 1	1, 2	20, 3
(14) 16, 7, 2	1, 1	8, 5	(32) 40, 23, 1	1, 2	20, 7
(15) 24, 7, 1	2, 1	24, 5	(33) 40, 23, 5	1, 2	20, 13
(16) 24, 7, 2	1, 1	24, 13	(34) 40, 23, 5	1, 2	20, 17
(17) 24, 7, 2	3, 1	24, 11	(35) 48, 31, 1	18, 1	24, 13
(18) 24, 7, 2	9, 1	24, 5			

give the residue $(*, q_0')_m$, since here p_0' does not occur. We are concerned therefore in this case with §1(3) for assigned values of a, b and primes $q \equiv q_0' \bmod m$; the corresponding values of n, r, c are useful only later in proving that the thirty-five shown in the table give instances of the theorems in §2 applied to §1(3).

From these we see, for example, from the second and third columns for (24), that

$$x^2 - 9y^2 - 2q^\beta z^2 = \mu^2,$$

in which the prime $q \equiv 5 \bmod 12$ has infinities of solutions in the sense of §1, with the properties stated in §2. By the first column the discriminant in this case is the class of all positive primes $\equiv 19 \bmod 24$. The list can be continued indefinitely, and likewise for the next two.

4. *Specific Theorem for* $\lambda = 0$, $s = 1$. As the case $\lambda = 0$ is not fundamentally different from $\lambda = 1$, we give but one example. The discriminant in the following is the class of all positive primes $\equiv 1 \bmod 8$; the primes p, q are both $\equiv 3 \bmod 8$:

$$x^2 - 2p^\alpha y^2 - q^\beta z^2 = \mu^2.$$

5. *Specific Theorems for* $\lambda = 1$, $s = 2$, $c_1 = c_2 = 1$. In each of the following the constant c is unity, so we shall not tabulate it. In the third column the significance of the parenthesis referring to values of q_0' is that one of the two values in the parenthesis is permissible for the accompanying modulus m. Thus we have the entry 40, (11, 19) in (4); hence q in

n, r_1, r_2	a, b	m, q_0'
(1) 8, 1, 3	1, 2	8, 5
(2) 24, 5, 5	12, 1	24, 13
(3) 24, 7, 7	12, 1	24, 13
(4) 40, 3, 7	10, 1	40, (11, 19)
(5) 40, 3, 23	10, 1	40, (11, 19)
(6) 40, 7, 27	10, 1	40, (11, 19)
(7) 40, 23, 27	10, 1	40, (11, 19)
(8) 120, 31, 31	60, 1	120, (61, 109)
(9) 120, 31, 79	60, 1	120, (61, 109)
(10) 120, 79, 79	60, 1	120, (61, 109)

§1(3) is a prime of one of the forms 11 or 19 mod 40 for this example. Since $c_1=c_2=1$ it is necesary in the first column, referring to the discriminant, to give only n, r_1, $r_2(c=1$, as stated).

These illustrate the fact that a given $[a, b, \lambda]$ may have, several discriminants. There are numerous examples in which $s>2$, but we shall omit these and pass to the proofs.

6. *Proofs.* All of the preceding results become obvious on combining two simple remarks. The notation is as in §§1, 2. Take for (T, U) the fundamental solution of the Pellian equation $t^2-Du^2=\mu^2$. Resolve D into the form $ap^\alpha\xi^2+bq^\beta\eta^2$, where ξ, η are integers >0. The rest follows at once. The resolution of D, combined with the successive solutions of the Pellian equation, obtained in the usual manner from (T, U), furnish the periods in §2. There are in each instance ω resolutions of D of the prescribed kind, and hence at least one. That such resolutions exist is known from the ingenious method of Bouniakowsky, or independently from the general arithmetical formulas obtained by paraphrasing identities between elliptic and theta functions. The latter method provides an inexhaustible source of these results and of others of a similar nature relating to forms in more than two variables. Bouniakowsky's method was exploited by Liouville; the specific theorems in §§3–4 can be verified by comparing with Liouville's resolutions of the corresponding D in volumes 3–5 of the second series of his Journal. I believe that proofs for these have not been published; on another occasion I will supply the details.

CALIFORNIA INSTITUTE OF TECHNOLOGY