QUARTIC CURVES MODULO 2*

BY

L. E. DICKSON

1. Introduction. Let f(x, y, z) be a homogeneous form of order n with integral coefficients. The points for which the three partial derivatives of f are congruent to zero modulo 2 shall be called derived points. A derived point shall be called a singular point or an apex of f = 0 according as it is or is not on f = 0. Apices do not arise if n is odd, since the left member of Euler's relation

$$x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + z\frac{\partial f}{\partial z} = nf$$

is zero at a derived point and therefore also f is zero. But if n is even, a derived point may not be on f = 0 and thus be an apex.

For example, any non-degenerate conic modulo 2 can be transformed linearly into $x^2 + yz = 0$. Its single derived point (100) is an apex.

Quartic curves modulo 2 have the remarkable property of possessing at most seven bitangents (or an infinity in a special case), whereas an algebraic quartic curve possesses twenty-eight in general. For the special quartic β of § 4, any line through the apex (001) is a bitangent, just as any line through the apex of the conic $x^2 + yz = 0$ is a tangent.

The number of non-equivalent types of quartic curves containing 0, 7, 6 real points and having no real linear factor is 8, 1, 6, respectively. In each case, the types are completely distinguished by the number and reality of the singular points and apices. Except for two types, in which there are only two bitangents and only two derived points, the intersections of the bitangents coincide completely with the derived points. The problem is more complicated in the case of quartic curves with five real points, there being twenty-five types (§ 7). Quartics with 1, 2, 3, or 4 real points have not been treated since they would probably not present sufficient novelty to compensate for the increased length of the investigation.

2. Bitangents. The general quartic is

$$Q = ax^4 + by^4 + cz^4 + dx^3y + exy^3 + fx^3z + gxz^3 + hy^3z + iyz^3 + jx^2y^2 + kx^2z^2 + ly^2z^2 + mx^2yz + nxy^2z + pxyz^2.$$

^{*} Presented to the Society (San Francisco Section), October 24, 1914.

Either (I) $d \equiv e \equiv f \equiv g \equiv h \equiv i \equiv 0 \pmod{2}$ or, after permuting the variables, we may assume that $d \equiv 1 \pmod{2}$. In the latter case we replace x by x + ey and obtain a Q with d = 1, e = 0. Replacing y by y + fz, and x by x + mz, we have also f = m = 0. In this case (II), d = 1, e = f = m = 0, the line x = ry + sz is a bitangent to Q if the quartic in y and z obtained by eliminating x is a perfect square, i. e., has no terms in y^3z and yz^3 ; the conditions are

$$r^2 s + nr + h = 0$$
, $s^3 + ps + gr + i = 0$.

If $g \equiv 1 \pmod{2}$, there are at most 7 sets of solutions r, s. Next, let $g \equiv 0 \pmod{2}$. Any root $\neq 0$ of the cubic in s leads to at most two r's. For i = 0 the root s = 0 leads to an infinitude of r's if and only if n = h = 0. In this case (II), $y = \rho z$ is a bitangent if and only if $\rho = 0$, g = 0, while z = 0 is not a bitangent. There are at most seven bitangents in case (II), unless g = i = h = n = 0, when there is an infinitude of bitangents, viz., all lines through (001).

For case (I), z = 0 is a bitangent; also $y = \rho z$ if and only if $n\rho^2 + p\rho = 0$; while x = ry + sz is a bitangent only when

$$mr^2 + nr = 0$$
, $ms^2 + ps = 0$.

In case (I), there is an infinity of bitangents if two of the coefficients m, n, p are zero, otherwise at most seven.

3. Real Points on the Quartic. The seven real points (i. e., with integral coördinates) modulo 2 are

$$1 = (100),$$
 $2 = (010),$ $3 = (001),$ $4 = (110),$ $5 = (101),$ $6 = (011),$ $7 = (111).$

The values of Q at these points are respectively

$$a, b, c,$$
 $a+b+d+e+j,$ $a+c+f+g+k,$ $b+c+h+i+l,$ and the sum of the fifteen coefficients.

4. Quartic Curves Without Real Points. The seven values in § 3 are now unity, so that

$$a = b = c = 1$$
, $j = d + e + 1$, $k = f + g + 1$, $l = h + i + 1$, $p = m + n + 1$.

(I) Consider case (I) of § 2. If m and n are not both zero, we may set m = 1, after interchanging x and y if necessary. If m = n = 1, we get

$$\alpha \, = \, x^4 \, + \, y^4 \, + \, z^4 \, + \, x^2 \, y^2 \, + \, x^2 \, z^2 \, + \, y^2 \, z^2 \, + \, x^2 \, yz \, + \, xy^2 \, z \, + \, xyz^2 \, ,$$

which is invariant under all real linear transformations. Its bitangents are the seven real lines. Their intersections, the seven real points, are apices and give all the apices. There is no singular point.

If m = 1, n = 0, we interchange x and z and have the case m = n = 0, viz.,

$$\beta = x^4 + y^4 + z^4 + x^2 y^2 + x^2 z^2 + y^2 z^2 + xyz^2.$$

The only bitangents are y = 0, z = 0 and x = ry, where r is arbitrary. Their intersections are 1, 3, and $(r \ 1 \ 0)$, all being apices except the last for $r^2 + r + 1 = 0$, when $(r \ 1 \ 0)$ is a singular point. There are no further derived points. Any line through apex 3 is a bitangent.

- (II) Consider case (II) of § 2, viz., d = 1, e = f = m = 0.
- (1) First, let h = 1. If n = 1, we replace y by y + x and then x by x + z and obtain a quartic with h = 1, n = 0, viz.,

$$\gamma_{g,i} = x^4 + y^4 + z^4 + x^3y + gxz^3 + (g+1)x^2z^2 + y^3z + iyz^3 + iy^2z^2 + xyz^2$$
.

By § 2, the bitangents are y = 0 (if g = 0) and

$$x = ry + sz$$
, $r^2 s = 1$, $s^3 + s + gr + i = 0$.

If g = i = 0, the bitangents are y = 0 and x = y + z, crossing at the apex 5; the only further derived point is the apex 3.

If g = 0, i = 1, the bitangents are y = 0, x = (s + 1)y + sy, where $s^3 + s + 1 = 0$; they intersect at the apices 7 and (s01). There is no further derived point.

If g = 1, i = 0, the seven bitangents are

$$x = ry + r^{-2}z$$
, $r^7 + r^4 + 1 \equiv 0 \pmod{2}$.

Replacing r by another root r^2 of this irreducible congruence, we obtain a bitangent meeting the former at $P = (\eta^3 \eta 1)$, where $\eta = r^6 + r^2 + 1$ is a root of $\eta^7 + \eta + 1 = 0$. The seven roots of the latter are obtained by replacing r by r^2 in succession in η , the resulting function, etc. These seven apices P are the only derived points.

If g = i = 1, the bitangents are

$$x = ry + r^{-2}z$$
, $r = 1$, $r^2 + r + 1 = 0$ or $r^4 + r^3 + 1 = 0$.

Their intersections are seen to be the apex 6 and the singular points

$$(y^3 + y, y, 1),$$
 $y^2 + y + 1 = 0,$ or $y^4 + y + 1 = 0.$

There are no further derived points.

(2) Second, let h = g = 0. If n = 1, i = 0, we replace x, y, z by y, x + z, x and then x by x + y and get γ_{00} . If n = i = 0, we replace z by z + x and have case (I). If n = 0, i = 1, we replace x by x + y, z by z + y, and get γ_{01} . If n = i = 1, we have

$$\delta = x^4 + y^4 + z^4 + x^3 y + x^2 z^2 + yz^3 + xy^2 z.$$

By § 2, its bitangents are y = 0, x = z, x = sz, x = y + z, $x = s^{-1}y + sz$, where $s^2 + s + 1 = 0$. Their intersections are the apices 2, 5, 7 and the singular points (s01), $(s1s^2)$. There are no further derived points.

(3) Finally, let h=0, g=1. If i=0, we apply (xyz) and, in case n=0, also x'=x+z, and obtain case (1). Hence let i=1. Then, if n=0, we replace y by y+x and have case (2). But if n=1, we have

$$\epsilon = x^4 + y^4 + z^4 + x^3y + xz^3 + yz^3 + xy^2z.$$

By § 2, its bitangents are x = z, x = sz, $x = \sigma^{-1} y + \sigma z$, where

$$s^2 + s + 1 = 0$$
, $\sigma^4 + \sigma + 1 = 0$.

Their intersections are the apex 2 and the singular points $(1\tau 1)$ and $(\tau \sigma^3 1)$ where $\tau = \sigma + \sigma^2$ is a root of $\tau^2 + \tau + 1 = 0$. There are no further derived points.

The eight classes of quartic curves modulo 2 without real points are distinguished by the number and reality of their apices and singular points. These derived points coincide with the intersections of the bitangents, except for γ_{00} which has only two bitangents and two apices.

5. Quartic Curves Containing all Seven Real Points. The conditions are

$$a = b = c = 0$$
, $j = d + e$, $k = f + g$, $l = h + i$, $p = m + n$.

For case (I) of $\S 2$, Q is the product of four linear functions. For case (II),

$$Q = x^3y + x^2y^2 + gxz^3 + gx^2z^2 + hy^3z + iyz^3 + (h+i)y^2z^2 + nxy^2z + nxyz^2.$$

It has the factor x if h = i = 0, factor y if g = 0, factor x + y if i = 1, h = n, factor x + z if h = 0, n + i = 1, factor x + y + z if n = i, h + i = 1. We exclude these cases. Then, if n = 0, we have h = i = 1 and get

$$A = x^3 y + x^2 y^2 + xz^3 + x^2 z^2 + y^3 z + yz^3.$$

But, if n = 1, we have h = 1, i = 0; the resulting Q is derived from A by replacing x by y + z, y by x, z by y. The bitangents to A are

$$x = (s^3 + 1)y + sz, s^7 + s + 1 = 0.$$

Their intersections are the apices $(1z^3z)$, $z^7 + z^3 + 1 = 0$, which give all the derived points. The single type of irreducible quartic curve with seven real points has seven imaginary bitangents whose seven intersections are apices and give all the derived points.

6. Quartic Curves with Six Real Points. After applying a real transformation, we may assume that the curve contains the real points other than 1. Then

$$a = 1$$
, $b = c = 0$, $d + e + j = f + g + k = m + n + p = 1$, $l = h + i$.

(1) First, let d and f be not both zero. As in § 2, we may set d=1, e=f=m=0. Then Q has the factor x if h=i=0, factor x+y if h=n, g=i, factor x+z if h=0, n=i, factor x+y+z if h=n+1, g=i+n. We exclude these cases. Then if h=0, we have i=n=g=0, and get

$$B = x^4 + x^3 y + x^2 z^2 + yz^3 + y^2 z^2 + xyz^2.$$

Its four bitangents are y = 0 and x = sz, where $s^3 + s + 1 = 0$. Their intersections are the singular point 2 and the apices (s01). There are no further derived points.

Next, if h = n = 1, we have i = g + 1. According as g = 0 or g = 1, we get

$$C = x^4 + x^3 y + x^2 z^2 + y^3 z + y z^3 + x y^2 z$$
,

$$D = x^4 + x^3 y + xz^3 + y^3 z + y^2 z^2 + xy^2 z.$$

The seven bitangents to C are y = 0, x = ry + z, where $r^2 + r + 1 = 0$, and

$$x = \rho y + (\rho + \rho^3)z$$
, $\rho^4 + \rho^3 + 1 = 0$.

Their intersections are the singular point 5 and the apices (r01), and $(x1x^2)$ where $x^4 + x + 1 = 0$. There are no further derived points.

The seven bitangents to D are $x = s^3 y + sz$, $s^7 + s^3 + 1 = 0$. This meets the one with s replaced by the root s^2 in P = (x1z), where $x = s^5 + s^4$, $z = s^4 + s^3 + s^2$, so that $z = x^3$, $x^7 + x + 1 = 0$. All seven roots of the latter are obtained by replacing s by s^2 in succession in x, the resulting function, etc. These seven apices P give all the derived points of D.

Finally, if h=1, n=0, we have i=g+1. Then if g=0 the function is derived from B by the transformation x'=x+y, z'=z+y. If g=1, it is derived from D by z'=z+y.

(2) Second, let d = f = 0, while e and g are not both zero. Interchanging y and z, if necessary, we may set e = 1. We make h = n = 0 by use of x' = x + z and y' = y + z. We may set i = 1, g = m, since otherwise Q has the factor x, x + y, or x + y + z. According as m = 0 or m = 1, we have

$$E = x^4 + xy^3 + x^2z^2 + yz^3 + y^2z^2 + xyz^2$$
,

$$F = x^4 + xy^3 + xz^3 + yz^3 + y^2z^2 + x^2yz.$$

The only bitangents to E are y=0 and y=z. They intersect at the apex 1. The only further derived point is the singular point 5.

The seven bitangents to F are $y = \alpha z$, where $\alpha^3 = 1$, and

$$x = ry + r^2 z$$
, $r^4 + r + 1 = 0$.

Their intersections are the four singular points

$$(x, x^2 + x^3, 1), x^4 + x^3 + x^2 + x + 1 = 0,$$

and the apices 1 and (x, 1, 1), where $x^2 + x + 1 = 0$. There are no further derived points.

(3) Third, let d = f = e = g = 0. If m = 0, we make e = 1 by use of z' = z + y and have case (2). Henceforth, let m = 1. If n = 0, Q has the factor x + hy + iz. Hence we may set n = 1. If i = h = 0, Q has the factor x. In the contrary case, we interchange y and z and set h = 1. By use of y' = y + z, we make i = 0 and get

$$G = x^4 + x^2 y^2 + x^2 z^2 + y^3 z + y^2 z^2 + x^2 yz + xy^2 z + xyz^2$$
.

Its seven bitangents are y = 0, z = 0, y = z, x = ry, x = ry + z, where $r^2 + r + 1 = 0$. Their intersections are the singular points 3, 5 and the apices 1, (r10), (r11). There are no further derived points.

The six types of quartic curves containing six real points and having no linear factor are distinguished by the number of singular points and apices. These derived points coincide with the intersections of the bitangents, except for E which has only two bitangents and two derived points.

7. Quartic Curves with Five Real Points. The two real points not on the curve may be taken to be 1 and 2. Then

$$a = b = 1$$
, $c = 0$, $j = d + e$, $k = f + g + 1$, $l = k + i + 1$, $p = m + n$.

(I) Let d and e be not both zero. Interchanging x and y if necessary, we may set d=1. Applying x'=x+z and y'=y+z, we may set m=f=0 and get

$$q = x^{4} + y^{4} + x^{3} y + exy^{3} + (e + 1)x^{2} y^{2} + gxz^{3} + (g + 1)x^{2} z^{2} + hy^{3} z + iyz^{3} + (h + i + 1)y^{2} z^{2} + nxy^{2} z + nxyz^{2}.$$

A real transformation replacing q by a function of the same type must leave unaltered the line z=0 determined by the two real points 1 and 2. But z=0 meets q=0 at (x10), where $(x+1)^2(x^2+x+1)=0$ if e=1, and $(x+1)(x^3+x+1)=0$ if e=0; while z=0 meets Q with d=e=0 at (x10) where $(x+1)^4=0$. Hence quartics belonging to different ones of these three classes are not equivalent.

(I₁) Let e = 1. We may drop the case h = 1, n = 0; for, if we interchange x and y and then replace y by y + z, we obtain a q with the coefficients e' = 1, g' = i + 1, h' = 0, i' = g, n' = 1. If h = n, we may drop the case i = 0, g = 1; for, if h = n = 0, we have only to interchange x and y to permute

g and i; while, if h = n = 1, we replace x by y + z and y by x + z and obtain a like q with g and i permuted. We set

$$q = [ghin], \quad \mu = x^4 + y^4 + x^3y + xy^3.$$

The q's with a single singular point S and no apex are

$$[1010] = \mu + xz^3 + yz^3, \qquad S = 4;$$

$$[1001] = \mu + xz^3 + y^2z^2 + xy^2z + xyz^2, \qquad S = 6.$$

These are not equivalent since 1 and 2 are collinear with 4, but not with 6.

Those with exactly four derived points are

$$[1111] = \mu + xz^3 + y^3z + yz^3 + y^2z^2 + xy^2z + xyz^2, S = 4, 6, (11z),$$

$$z^2 + z + 1 = 0.$$

$$[0101] = \mu + x^2 z^2 + y^3 z + xy^2 z + xyz^2, \qquad S = 3, 4, 5, 7.$$

$$[0001] = \mu + x^2 z^2 + y^2 z^2 + xy^2 z + xyz^2, \quad S = 3, 5;$$

apices (01z),
$$z^2 + z + 1 = 0$$
.

$$[0010] = \mu + x^2 z^2 + yz^3$$
, $S = 4, 5$; apices (x01), $x^2 + x + 1 = 0$.

The last two are not equivalent, since 4 alone is collinear with 1, 2.

Those with one real and six imaginary derived points are

$$[0h11] = \mu + x^2 z^2 + hy^3 z + yz^3 + hy^2 z^2 + xy^2 z + xyz^2.$$

If h = 1, the only singular point is 4, while the apices are (z01), $(z^2 + 1$, 1, z), where $z^3 + z + 1 = 0$. If h = 0, the singular points are 7 and $(z^2 1z)$, where $z^3 + z^2 + 1 = 0$, while the apices are (x01), $x^3 + x + 1 = 0$.

The only q with seven imaginary derived points (apices A) is

$$[1011] = \mu + xz^3 + yz^3 + xy^2 z + xyz^2, \qquad A = \left(\frac{z^2}{z^2 + 1}, 1, z\right),$$
$$z^7 + z^6 + z^5 + z^3 + z^2 + z + 1 = 0.$$

There remains only [0000], which has the factor x + y.

 (I_2) Let e = 0. Write

$$q = (ghin), \quad \lambda = x^4 + y^4 + x^3 y + x^2 y^2.$$

The part λ of q free of z has the single real factor x+y. Hence the only possible real linear factors of q are x+y and x+y+z. The first is a factor if g=i, n=h; the second if g=i+h, n=h+1. After the exclusion of these cases, there remain only the following eight, for which all of the derived points are shown.

$$(0100) = \lambda + x^2 z^2 + y^3 z$$
, singular 3.

$$(1000) = \lambda + xz^3 + y^2z^2$$
, apex 2.

$$(1001) = \lambda + xz^3 + y^2z^2 + xy^2z + xyz^2$$
, singular 7, apices 2,

$$(01z), z^2 + z + 1 = 0.$$

$$(0010) = \lambda + x^2 z^2 + yz^3$$
, singular 5, apices 2, $(x01)$,

$$x^2+x+1=0.$$

To show that the last two are not equivalent, we consider the tangents at the real points of the curve other than 4 and the singular point. For the first,* the tangents at these points 3, 5, 6 are x = 0, x = z, x = 0; for the second, the tangents at 3, 6, 7 are y = 0, y = z, x = z and are distinct.

$$(0011) = \lambda + x^2 z^2 + yz^3 + xy^2 z + xyz^2, \quad \text{apices 2,} \quad (z01),$$

$$(z^2 1z)$$
, $z^3 + z + 1 = 0$.

$$(0111) = \lambda + x^2 z^2 + y^3 z + yz^3 + y^2 z^2 + xy^2 z + xyz^2, \quad \text{singular 6,}$$

$$\text{apices} \quad (x01), \quad x^3 + x + 1 = 0, \quad (z^2 + 1, 1, z),$$

$$z^3 + z^2 + 1 = 0.$$

$$(1110) = \lambda + xz^3 + y^3z + yz^3 + y^2z^2$$
, apices $(1 + z^{-2}, 1, z)$,

$$z^7 + z^4 + 1 = 0.$$

(1101) =
$$\lambda + xz^3 + y^3z + xy^2z + xyz^2$$
, apices $\left(\frac{1}{z^2 + 1}, 1, z\right)$,

$$z^7 + z^6 + z^5 + z^3 + z^2 + z + 1 = 0$$
.

To show that the last two are not equivalent, we employ the tangent at the point 4 uniquely determined by the real points 1 and 2. For the first, this tangent is x + y + z = 0; it meets the curve at 4, 5, 6; the tangent at 5 is x = z and meets the curve again at 7; the tangent at 6 is x = 0 and meets the curve again at 3. For (1101), the tangent at 4 is x = y, which meets the curve at 4, 3, 7; the tangents at 3 and 7 are x = 0 and y = z, each of which meets the curve again only at 6.

(II) Let d and e be zero, but f and h not both zero. After interchanging x and y if necessary, we may set f = 1, and then make g = 0 by use of x' = x + z. We get

^{*} Its bitangents are x = 0, x = z, $x = s^2 y + sz$, $s^2 + s + 1 = 0$. The bitangents to (0010) are y = 0, x = z, x = sz. In each case their intersections are the derived points.

$$Q = x^{4} + y^{4} + x^{3}z + hy^{3}z + iyz^{3} + (h + i + 1)y^{2}z^{2} + mx^{2}uz + nxu^{2}z + (m + n)xuz^{2}.$$

The possible real linear factors are x + y, x + y + z, occurring if

$$h = m + n + 1$$
, $i = 0$ or $i = n + 1$.

(II₁) Let m = 0, h = 1. We make i = 0 by use of y' = y + z. If n = 0, x + y is a factor. Hence we set n = 1 and get

$$x^4 + y^4 + x^3 z + y^3 z + xy^2 z + xyz^2$$
, singular 3, apices (x10), $(x^2 x^2)$, $x^3 + x + 1 = 0$.

(II₂) Let m = h = 0. We exclude the case i = 0, n = 1, when x + y is a factor. If n = i = 0, we have

 $x^4 + y^4 + x^3 z + y^2 z^2$, singular 3, 6, apices 2, (0y1), y any $\neq 0$, 1. If n = 0, i = 1, we have

$$x^4 + y^4 + x^3 z + yz^3$$
, apex 2 only derived point.

If n = i = 1, we have

 $x^4 + y^4 + x^3 z + yz^3 + xy^2 z + xyz^2$, singular 4, apices 2,

$$(1y1)$$
, $y^2 + y + 1 = 0$.

(II₃) Let m=1. We exclude the case h=n, i=0 or i=n+1, since Q then has the factor x+y or x+y+z. First, let n=0, h=1. The form with i=1 is obtained from that with i=0 by replacing x by x+z, y by y+z. In that with i=0 we interchange x and y and get the form in (II₁). Next, if n=h=i=1, we have

 $x^4 + y^4 + x^3 z + y^3 z + yz^3 + y^2 z^2 + x^2 yz + xy^2 z$, singular 4, no apex.

Finally, let n = 1, h = 0. If i = 0, we have

 $x^4 + y^4 + x^3 z + y^2 z^2 + x^2 yz + xy^2 z$, singular 3, apices 2,

$$(x10)$$
, $x^2 + x + 1 = 0$.

Replacing x by x + z, y by y + z, we obtain the form with i = 1.

(III) d=e=f=h=0. If m=n, g=i or g=i+n, Q has the factor x+y or x+y+z. First, let m and n be not both zero. Interchanging x and y, we may set m=1. If n=1, Q has a linear factor. If n=0, we make g=0 by use of y'=y+z. According as i=1 or i=0, we have

$$x^4 + y^4 + x^2 z^2 + yz^3 + x^2 yz + xyz^2$$
, apices 1, 2, (x01),
$$x^2 + x + 1 = 0;$$
 $x^4 + y^4 + x^2 z^2 + y^2 z^2 + x^2 yz + xyz^2$, singular 3, 5, apices 1, 2.

Second, let m = n = 0. There is a linear factor if g = i. In the contrary case we interchange x and y and have g = 1, i = 0, and get

$$x^4 + y^4 + xz^3 + y^2z^2$$
, singular 4, apices 2, (1y0), y any ± 1 .

The only types in (II) and (III) for which there is the same number of singular points and same number of apices are the last ones in (II₂) and (II₃). These are not equivalent since the real points 1 and 2, not on the curve, are collinear with the singular point 4 of the first curve, but not with that of the second.

The 25 types of quartic curves containing the five real points other than 1 and 2, and having no real linear factor, are distinguished by the number and reality of their singular points and apices, and their relation to the line joining 1 and 2, together with properties of the tangents at the real points in the cases of two pairs of quartics in (I_2) .

THE UNIVERSITY OF CALIFORNIA, October, 1914.