ACTA ARITHMETICA
XCIX.1 (2001)

Constructions of plane curves with many points

by

F. Rodríguez Villegas (Austin, TX), J. F. Voloch (Austin, TX)
and D. Zagier (Bonn)

In this paper we investigate some plane curves with many points over $\mathbb{Q}$, finite fields and cyclotomic fields.

In a previous paper [5] the first two authors constructed a sequence of absolutely irreducible polynomials $P_d(x,y) \in \mathbb{Z}[x,y]$ of degree d having low height and many integral solutions to $P_d(x,y) = 0$. (The definition of these polynomials will be recalled in Section 4.) Here we construct further examples of polynomials of arbitrarily large degree d over $\mathbb{Q}$ with many rational zeros, improving the known record for the maximal number of rational zeros of a smooth polynomial in two variables over $\mathbb{Q}$ of given large degree. We also construct examples of two variable polynomials having the maximal theoretically possible number of zeros at roots of unity and over finite fields. Finally, we return to the polynomials P_d and show that for certain special values of d they have a few more zeros than were found there.

Here is a more precise statements of the results obtained, with a few remarks about each one.

Theorem 1. *For each natural number m, the plane projective curve of degree m defined by the vanishing of the polynomial*

$$G_m(x,y,z) = \sum_{\substack{i,j,k\geq 0\\ i+j+k=m}} x^i y^j z^k \tag{1}$$

is non-singular in characteristic 0 or characteristic $p \nmid (m+1)(m+2)$, and has zeros at $2m^2$ points where the coordinates x, y and z are roots of unity.

The polynomials G_m, which are in some sense the simplest imaginable homogeneous polynomials of degree m (all coefficients are equal!), simultaneously achieve the optimum for two different problems relating to the number of zeros of a polynomial in two variables: On the one hand, a simple argu-

2000 *Mathematics Subject Classification*: 14G05, 11G30.

ment (given in Section 1) shows that no non-reciprocal plane curve of degree m can vanish at more than $2m^2$ points whose coordinates are roots of unity. On the other hand, Theorem 0.1 of [7] tells us that an absolutely irreducible plane curve of degree $1 < d < p$ defined over $\mathbb{F}_p$ has at most $d(d+p-1)/2$ points over $\mathbb{F}_p$, and, as we will check in Section 1, Theorem 1 implies that the curve $G_m(x^k, y^k, z^k) = 0$ with $p - 1 = (m+2)k$ attains this bound.

THEOREM 2. *For any integer d divisible by 6 there exist infinitely many polynomials $F(x,y) \in \mathbb{Q}[x,y]$ of degree d of the form*

$$F_d(x,y) = (f(h(x)) - f(h(y)))/(h(x) - h(y))$$

such that the curve $F_d(x,y) = 0$ is smooth and contains at least $d^2 + 6d$ rational points.

These are, for large d, the smooth polynomials in two variables with the largest number of points over $\mathbb{Q}$ known. We refer the reader to the introduction of [5] for references to some speculations as to whether there is a uniform bound on the number of rational points on a curve of fixed genus (see also [3]). We note that there are constructions, due to Brumer, Harris and Mestre (see [3] or [4]) which lead to curves with many points over number fields. For instance, Harris obtains plane curves of degree d with $3d^2$ rational points over cyclotomic fields. Brumer and Mestre construct hyperelliptic curves of any genus g with $16(g+1)$ rational points over the field of $(g+1)$st roots of unity and $8g + 12$ points over $\mathbb{Q}$. The curves of Brumer and Mestre all have large automorphism groups. Silverman has suggested that one should measure the number of points divided by the order of the automorphism group. From this point of view the curves occurring in Theorem 2 are good, since they usually have the involution $(x,y) \mapsto (y,x)$ as their only non-trivial automorphism, and the curves constructed in [5] are still better, since they probably have no non-trivial automorphisms at all. Here we will obtain:

THEOREM 3. *For infinitely many values of d, the equation $P_d(x,y) = 0$ of degree d has at least $d^2 + 2d + 8$ integral solutions.*

This improves (for some d) the result of [5], where it was shown that $P_d = 0$ has at least $d^2 + 2d + 3$ integral solutions for every d. We will also show that the number "$d^2 + 2d + 8$" in Theorem 3 can be increased by 1 if we allow rational zeros, and will give numerical evidence suggesting that in general there are very few, if any, further rational zeros.

1. Variations of a construction of Schaefer. A very simple construction of two-variable polynomials with many integral zeros was suggested by Ed Schaefer: if $f(x) \in \mathbb{Z}[x]$ has distinct integer roots, say $\alpha_1, \ldots, \alpha_n$, then the polynomial $f(x) + \lambda f(y)$, which is irreducible for generic λ, has degree

$d = n$ and n^2 integral roots at $(x, y) = (\alpha_i, \alpha_j)$. To improve this, take $\lambda = -1$. The polynomial $f(x) - f(y)$ now has the linear factor $x - y$. If we remove it, then the quotient is usually irreducible, has degree $d = n-1$, and has $n^2-n = d^2 + d$ roots $(x, y) = (\alpha_i, \alpha_j)$, $\alpha_i \neq \alpha_j$, which is slightly better in terms of the degree. If f is also assumed to be even, then $f(x) - f(y)$ is divisible by $x^2 - y^2$ and the quotient has degree $d = n - 2$ and $n(n-2) = d^2 + 2d$ roots, very nearly as good as the number d^2+2d+3 found in [5] for the polynomials P_d, and this can be improved still further in some cases, as we will see below.

First, however, we look at a generalization of this construction, replacing "even" by "invariant under multiplying x or y by ζ, where ζ is a kth root of unity." This of course requires working over a field K which contains the kth roots of unity, so no longer applies to $\mathbb{Q}$, but will be of interest in the cases of cyclotomic and of finite fields. Let K be such a field and set $f(x) = \prod(x^k - \alpha_i^k)$, where $\alpha_1, \ldots, \alpha_r$ are elements of $K^\times$ whose kth powers are distinct. Then the polynomial $P(x, y) = (f(x) - f(y))/(x^k - y^k)$ has degree $d = k(r-1)$ and vanishes on the $k^2r(r-1)$ points $(\zeta\alpha_i, \zeta'\alpha_j)$, where ζ, ζ' are kth roots of unity and $i \neq j$. Thus we get polynomials of degree d with $d^2 + kd$ points over any number field containing the kth roots of unity, though it is unclear how good these examples really are.

More interesting is what the construction gives in the case of finite fields. Let p be a prime and k a divisor of $p - 1$, $k < (p-1)/2$. Let $r + 1 = (p-1)/k$. We then get polynomials of degree $d = p - 1 - 2k$ with $d^2 + kd = d(d + p - 1)/2$ points over $\mathbb{F}_p$, and this achieves the upper bound from [7] mentioned in the introduction, provided we know that our polynomials are absolutely irreducible. This information is given by Theorem 1 in the case of the polynomial

$$f(x) = (x^{(m+2)k} - 1)/(x^k - 1),$$

since then $P(x, y) = G_m(x^k, y^k, 1)$, with $G_m(x, y, z)$ as in equation (1), so that in this case we indeed achieve the theoretical upper bound (with $d = mk$ and zeros at all $x, y, z \in \mathbb{F}_p^\times$ with x^k, y^k and z^k distinct).

As was also mentioned in the introduction, the same polynomials G_m also achieve the maximum for the number of zeros at roots of unity of a non-reciprocal polynomial of degree m over $\mathbb{Q}$, or indeed even over $\mathbb{R}$. To see this, let $h(x, y) = 0$ be such a polynomial. If we have a solution of $h(\zeta, \zeta') = 0$ with ζ and ζ' roots of unity, then taking complex conjugates we get $0 = h(\overline{\zeta}, \overline{\zeta'}) = h(\zeta^{-1}, \zeta'^{-1})$. Thus (ζ, ζ') is also a point on the curve $(xy)^m h(x^{-1}, y^{-1})$, of degree $2m$. If those two curves have no component in common, there can be only $2m^2$ points in their intersection; we call such polynomials h or the curves that they define *non-reciprocal*. For example, if h is smooth and does not go through the origin then h is non-reciprocal. (For bounds for general curves see [6].)

In this connection we also mention the recent paper [1], in which the authors not only also give the upper bound $2m^2$ for the number of "cyclotomic" points on non-reciprocal plane curves and show (with a different example) that it is best possible, but also prove a theorem implying the upper bound $(22/3)m^2$ for the number of cyclotomic points on an arbitrary plane curve of degree m which has no components in common with any curve of the form $x^a y^b = 1$ $(a, b \in \mathbb{Z})$.

2. Construction of curves with many points over $\mathbb{Q}$. Returning to the case of $\mathbb{Q}$ and to $P(x, y)$ of the form $(f(x) - f(y))/(x^2 - y^2)$ where f is an even polynomial of degree $d + 2$ with distinct integral roots, we can try to improve our lower bound $d^2 + 2d$ on the number of zeros of P by looking for solutions of the equation $f(x) = f(y) \neq 0$. We list only some first attempts in that direction; looking for better examples is an amusing game and the reader may want to play.

The idea is that if $f(x)$ has one or several blocks of zeros in arithmetic progression, then for certain small values of δ the difference $f(x) - f(x + \delta)$ has so many known zeros (corresponding to x where $f(x) = f(x + \delta) = 0$) that the remaining ones are the roots of a polynomial of small degree which may then split completely over $\mathbb{Q}$. There are many possible variants. For instance, if we take f to have its positive roots at $a, a + 1, \ldots, a + n - 1$ for some a and n, then $f(x + 1) = f(x)$ has only the obvious roots but

$$\frac{f(x+1)}{f(x-1)} = 1 + 4nx \frac{x^2 - a^2 - (n-1)(a-1/2)}{(x+a)(x+a-1)(x-a-n)(x-a-n+1)},$$

so if we arrange for $\kappa := a^2 + (n-1)(a-1/2)$ to be a perfect square, which is easy to do, then we get eight additional roots $(\pm\sqrt{\kappa} - 1, \pm\sqrt{\kappa} + 1)$, $(\pm\sqrt{\kappa} + 1, \pm\sqrt{\kappa} - 1)$ of the polynomial $(f(x) - f(y))/(x^2 - y^2)$. (Here a can even be a rational number, since we can always rescale x and y to get integral roots.) If we take instead f with its positive roots at $1, 3, \ldots, 2k-1$ and $2b + 1, 2b + 3, \ldots, 2b + 2l - 1$ for some positive integers k, l and some integer or rational number b, then we find

$$\frac{f(2x+1)}{f(2x-1)} = 1 + 2 \frac{(k+l)x^2 - kb(b+l)}{(x-k)(x-b-l)(x+b)},$$

so whenever $kb(b + l)/(k + l)$ is a perfect square we again get 8 extra roots. Finally, if we choose f with its positive roots at $1, 3, \ldots, \widehat{2r-1}, \ldots, 2n-1$ for some $0 < r < n$, then the non-trivial roots of $f(x + 1) = f(x - 1)$ and of $f(x + 2) = f(x - 2)$ are given by $(n-1)x^2 = 4nr(r-1)$ and $(n-1)x^2 = 4n^2 + (4r^2 - 4r - 3)n - 1$, respectively, and there are many pairs (n, r) for which one of these two equations has rational solutions, although unfortunately (at least up to $n = 1000$) none where they both do.

Summarizing, for each degree d there are infinitely many two-variable polynomials of degree d of the form $(f(x)-f(y))/(x^2-y^2)$ having at least d^2+2d+8 integral zeros.

It is easy to check that for generic even polynomials f which split completely over $\mathbb{Q}$, the curve defined by $(f(x)-f(y))/(x^2-y^2)=0$ is smooth. Thus we can guarantee that polynomials in the above result are smooth at the expense of reducing the number of points to d^2+2d.

We can construct polynomials with at least d^2+3d integral zeros, for all d divisible by 3, as follows. Let $h(x)=x^3-x^2$. It can easily be shown that there exist infinitely many rational numbers α such that $h(x)+\alpha$ splits completely in $\mathbb{Q}$. Let $\alpha_1,\dots,\alpha_n$ be distinct rational numbers such that $h(x)+\alpha_i$ splits into three distinct linear factors in $\mathbb{Q}$. Let $f(x)=\prod(h(x)+\alpha_i)$ and $F(x,y)=(f(x)-f(y))/(h(x)-h(y)), d=3n-3$. If $\beta_{ij}, j=1,2,3$, are the roots of $h(x)+\alpha_i=0, i=1,\dots,n$, then $F(x,y)=0$ contains the rational points $(\beta_{ij},\beta_{i'j'})$, $i,i'=1,\dots,n$, $i'\neq i$, $j,j'=1,2,3$. These points number $9n(n-1)=d^2+3d$, as claimed.

A slight modification of the same idea gives Theorem 2, which we now proceed to prove.

Proof of Theorem 2. Set $h(x)=x^6-2x^4+x^2$ and

$$C(\lambda)=\frac{(\lambda(\lambda-1)(\lambda+1)(2\lambda-1)(\lambda-2))^2}{(\lambda^2-\lambda+1)^6}.$$

Then the polynomial $h(x)-C(\lambda)$ splits as $\prod_{\alpha\in S(\lambda)}(x-\alpha)$ with

$$S(\lambda)=\left\{\pm\frac{\lambda^2-1}{\lambda^2-\lambda+1},\pm\frac{\lambda^2-2\lambda}{\lambda^2-\lambda+1},\pm\frac{2\lambda-1}{\lambda^2-\lambda+1}\right\}.$$

Now let $\lambda_1,\dots,\lambda_n$ be rational such that the $C(\lambda_i)$ are all distinct and set $f(X)=\prod_i(X-C(\lambda_i))$ and $F(x,y)=(f(h(x))-f(h(y)))/(h(x)-h(y))$. This polynomial has degree $d=6n-6$ and vanishes for $x\in S(\lambda_i)$, $y\in S(\lambda_j)$ with $1\leq i\neq j\leq n$, i.e., at $36n(n-1)=d^2+6d$ rational points. Finally, the curve defined by $F(x,y)=0$ is smooth for almost all $(\lambda_1,\dots,\lambda_n)\in\mathbb{Q}^n$ because, as is easily seen, the set of (complex) n-tuples $(\lambda_1,\dots,\lambda_n)$ for which this curve is smooth is Zariski open.

3. Proof of Theorem 1. Let m be a natural number and consider the homogeneous polynomial $G_m(x,y,z)$ defined in the introduction. By summing a geometric series, we can write it in the form

$$G_m(x,y,z)=\frac{1}{x-y}\left(\frac{x^{m+2}-z^{m+2}}{x-z}-\frac{y^{m+2}-z^{m+2}}{y-z}\right), \tag{2}$$

which is the form which was used in Section 1. Writing it this way makes it clear that we have not merely the m^2+m roots of $G_m(\zeta,\zeta',1)=0$ given

by taking ζ and ζ' to be distinct $(m+2)$nd roots of unity different from 1, but also the m^2-m roots of $G_m(\zeta,\zeta',1)=0$ given by taking ζ and ζ' to be distinct $(m+1)$st roots of unity different from 1. This proves the second assertion of the theorem.

To prove the first, we note that (2) can be rewritten as $G_m = D_{m+2}/D_2$, where

$$D_n = D_n(x,y,z) = \begin{vmatrix} 1 & 1 & 1 \\ z & x & y \\ z^n & x^n & y^n \end{vmatrix}. \tag{3}$$

From now on we fix m and write simply G for $G_m(x,y,1)$ and D for $D_{m+2}(x,y,1)$. Our first claim is that

$$\mathrm{Res}_x(G, \partial G/\partial y) = g(y)^{m-1}, \tag{4}$$

where Res_x denotes the resultant as polynomials in x and $g(y) = G(y,y) = \sum_{j=0}^{m}(j+1)y^j$. To prove this, we have to look at the simultaneous zeros of G and $G_y = \partial G/\partial y$. It is easy to deal with the points where $D_2 = 0$. Ignoring them, we have that the equations $G = G_y = 0$ are equivalent to $D = D_y = 0$. The polynomial D is the determinant of the matrix with columns $v(1)$, $v(x)$ and $v(y)$, where $v(x) := (1, x, x^{m+2})^t$, and similarly D_y is the determinant of the matrix with columns $v(1)$, $v(x)$, and $v'(y) = (0, 1, (m+2)y^{m+1})^t$. If both vanish, then all four vectors $v(1)$, $v(x)$, $v(y)$ and $v'(y)$ must lie in the same two-dimensional space. (It cannot be one-dimensional since $v(y)$ is never proportional to $v(1)$ for $y \neq 1$.) In particular this holds for $v(1)$, $v(y)$ and $v'(y)$, so the determinant they define is zero, and this determinant is simply $g(y)$. Hence any zero of $G = G_y = 0$ has y-coordinate equal to one of the roots $y_1, \ldots, y_m$ of $g(y) = 0$, and conversely each of these roots occurs as the y-coordinate of precisely $m-1$ zeros of $G = G_y = 0$. (Up to a scalar, the unique vector orthogonal to $v(1)$, $v(y_i)$ and $v'(y_i)$ is $w(y_i) = ((m+1)y_i^{m+2}, -(m+2)y_i^{m+1}, 1)$, so the roots of $G(x,y_i) = G_y(x,y_i) = 0$ are the roots of the polynomial

$$(x^{m+2} - (m+2)y_i^{m+1}x + (m+1)y_i^{m+2})/((x-1)(x-y_i)^2)$$

of degree $m-1$.) This proves equation (4) up to a constant, which can then be shown to be 1 by looking at the terms of highest degree.

Now to find the possible singular points of the projective curve C, we must look for the common zeros of G, G_x, and G_y and hence, by (4), of G_x and g. Again we can ignore the zeros of D_2 and the points at infinity, which are easily dealt with. Then $G = G_x = G_y = 0$ is equivalent to $D = D_x = D_y = 0$. At a simultaneous zero of G, G_x, and G_y, all five vectors $v(1)$, $v(x)$, $v'(x)$, $v(y)$ and $v'(y)$ must be in the same 2-dimensional space. By the argument already given, the orthogonal complement of this space is spanned by the vector $w(y)$, and by symmetry it is also spanned by

$w(x)$, so these two vectors must be equal. Subtracting them, we find that $(m+1)(x^{m+2}-y^{m+2})$ and $(m+2)(x^{m+1}-y^{m+1})$ both vanish, and this is clearly impossible if $m+1$ and $m+2$ are non-zero. Therefore singularities can only occur in characteristics dividing $(m+1)(m+2)$, as claimed.

REMARKS. 1. We have observed numerically the following identity, which would also imply the statement about non-singularity in Theorem 1, but were unable to prove it:

$$\mathrm{Res}_y(\mathrm{Res}_x(G, \partial G/\partial x), g) = 2^{-m}(m+1)^{m^2-2m+2}(m+2)^{m^2-m}.$$

2. In our previous example over finite fields we only considered the points on $G(x^k, y^k) = 0$ above the $(m+2)$nd roots of unity, but we can also consider the $(m+1)$st by, for example, taking $p-1 = k(m+1)$. Incidentally, $G(0,\zeta) = 0$ if $\zeta \neq 1$ is an $(m+1)$st root of unity and there are similar points also on the lines $y = 0$ and $z = 0$. So $G(x^k, y^k) = 0$ in this case has $k^2m(m-1) + 3km$ rational points over $\mathbb{F}_p$. This again attains the bound of Theorem 0.1 of [7] if $k = 2$, and comes fairly close for other small k. It also has the feature that we can obtain curves of odd degree, which we could not do in the previous example. One can also try to use simultaneously at least some of the $(m+1)$st and $(m+2)$nd roots of unity, but we did not obtain interesting examples this way.

4. Integral points on the curve $P_d(x,y) = 0$. In [5], certain polynomials $P_d(x,y) \in \mathbb{Z}[x,y]$ of degree d were constructed and it was shown that P_d for every d is absolutely irreducible and has at least $d^2 + 2d + 3$ integral solutions to $P_d(x,y) = 0$. In his review [2] of [5] for Math. Reviews, A. Bremner pointed out that in fact one family of integral solutions had been missed and that in fact the equation $P_d(x,y) = 0$ has at least $d^2 + 2d + 4$ integral solutions when d is odd. This prompted us to look again for patterns in the extra points we found experimentally which might occur for infinitely many, but not all, d. This section reports our findings.

The polynomials P_d can be defined by $P_d(-X, Y^2) = T_{2d}(X, Y)$, where the $T_k[X,Y] \in \mathbb{Z}[X,Y]$ $(k = 0, 1, \ldots)$ are given by the generating function

$$H(t) := (1-t)^r(1+t)^s = \sum_{k=0}^{\infty} T_k(-r-s, -r+s)\,\frac{t^k}{k!} \tag{5}$$

or—expanding by the binomial theorem—more explicitly by

$$T_k(-r-s, -r+s) = k! \sum_{n=0}^{k} (-1)^n \binom{r}{n}\binom{s}{k-n}. \tag{6}$$

We now describe ten constructions of infinite families of integer solutions of $P_d(x,y) = 0$. The first four are the ones already given in [5], but we re-prove

them here for completeness and also because the proofs here, based on the generating function (5), are in some cases shorter than those in [5]. The fifth family gives the extra solution for odd d observed by Bremner, and the first seven together give (for suitable d) the conclusion of Theorem 2.

(I) *r and s small.* If r and s are non-negative integers, then $H(t)$ is a polynomial of degree $r+s$, so $T_k(-r-s,-r+s)$ vanishes for $k > r+s$. This gives us the $d(d+1)$ integral zeros $(x,y) = (n,m^2)$ of $P_d(x,y) = 0$, where $0 \le m \le n \le 2d-1$, $m \equiv n \pmod 2$.

(II) *$x = 4d$.* If r and s are positive odd integers with sum $2k$, then the coefficients of the polynomial $H(t)$ are anti-symmetric (i.e. $t^{2k}H(1/t) = -H(t)$), so its middle coefficient vanishes. For P_d this gives the d additional zeros $P_d(4d, 4n^2) = 0$ for $0 < n < 2d$, n odd.

(III) *$y = 9$.* A further zero $P_d(8d+1, 3^2) = 0$ can be seen as follows. Take $r = 4d-1$, $s = 4d+2$ in (5). Then $H(t) = (1+t)^3(1-t^2)^{4d-1}$, and the coefficient of t^{2d} in this is, up to sign, equal to $\binom{4d-1}{d} - 3\binom{4d-1}{d-1}$, which indeed vanishes.

(IV) *$x = 2d-3$ or $2d-4$.* The generating function identity (5) and the obvious differential equation

$$\frac{H'(t)}{H(t)} = -\frac{r}{1-t} + \frac{s}{1+t}$$

imply the recursion $T_{k+1} = YT_k + k(X+k-1)T_{k-1}$ for the polynomials $T_k(X,Y)$. (This recursion, with suitable initial conditions, was in fact taken as the definition of T_k in [5].) For the subfamily $P_d(x,y) = T_{2d}(-x, \sqrt{y})$ this leads to the recursion

$$\begin{aligned} P_{d+1} = {} & [y - (4d+1)x + 8d^2]P_d \\ & - [2d(2d-1)(x-2d+1)(x-2d+2)]P_{d-1}. \end{aligned}$$

The two coefficients in square brackets vanish if x equals $2d-1$ or $2d-2$ and $y = (4d+1)x - 8d^2$, giving two additional integer zeros.

(V) *$x = 4d-3$.* For d odd we have a further solution $P_d(4d-3, (2d-1)^2) = 0$. (These are the points noticed by Bremner.) To prove this we must show that the coefficient of t^{2d} in $H(t)$ is zero when $r = d-1$, $s = 3d-2$. For these values of r and s, $H(t) = (1-t^2)^{d-1}(1+t)^{2d-1}$, so the coefficient in question is $\sum_{n=1}^{d-1}(-1)^{d-n}\binom{d-1}{d-n}\binom{2d-1}{2n}$, which vanishes if d is odd because the terms for n and $d-n$ cancel.

(VI) *$r = 2$.* For $r = 2$ the function $H(t)$ in (5) equals $(1+t)^{s+2} - 4t(1+t)^s$, so

$$\begin{aligned} T_k(-s-2, s-2) &= k!\left[\binom{s+2}{k} - 4\binom{s}{k-1}\right] \\ &= \frac{1}{4}s(s-1)\dots(s-k+3)[(2s-4k+3)^2 - (8k+1)]. \end{aligned}$$

The zeros at $s = 0, 1, \ldots, k-3$ correspond to construction (I), but if $k = 2d$ and $16d + 1 = a^2$ for some integer a then we get a new integral point

$$x = \left(\frac{a+1}{2}\right)^2, \quad y = \left(\frac{a+5}{2}\right)^2 \left(\frac{a-3}{2}\right)^2$$

on $P_d(x, y) = 0$. In fact we get *two* new solutions, since we can replace a by its negative.

(VII) $r = 3, 4, 5$. More generally, if r is a fixed positive integer then for $k \geq r$ the sum in (6) terminates at $n = r$ and can be rewritten as $\binom{k}{r}^{-1}\binom{s}{k-r}Q_r(k, s)$ with

$$Q_r(k, s) = r! \sum_{n=0}^{r} (-1)^n \binom{k}{n} \binom{r+s-k}{r-n} \in \mathbb{Z}[k, s],$$

a polynomial of degree r. For r odd, we set $\widetilde{Q}_r(k, s) = Q_r(k, s)/(r + s - 2k)$ to remove the factor corresponding to (II) above. Then for $r = 3$ we find

$$4\widetilde{Q}_3(k, s) = (2s - 4k + 3)^2 - (24k + 1)$$

and hence two further integral solutions of $P_d = 0$ whenever $48d + 1$ is a square. (This case is very similar to (VI), but has been listed separately for convenience in counting solutions below.) For $r = 4$ or 5, we find

$$Q_4(k, t + 2k - 4) = 3(2k - t^2 + t - 1)^2 - (2t^4 - 2t^2 + 3),$$
$$3\widetilde{Q}_5(k, t + 2k - 5) = 5(6k - t^2 + 3t - 5)^2 - (2t^4 - 10t^2 + 53),$$

each giving only a finite number of further solutions corresponding to the integral points on an elliptic curve of positive rank over $\mathbb{Q}$.

(VIII) $x = 2d+2$. Another infinite family of integral zeros of $P_d(x, y) = 0$ for special d is given by $d = 2c^2 - 1$, $x = y = 4c^2$ with $c \in \mathbb{N}$. This solution is found by going back to the argument for construction (I) and considering the coefficient of t^{r+s-2} in $H(t)$.

(IX) $x = 2d+3$. Similarly, if we look at the coefficient of t^{r+s-3} in $H(t)$, then after removing from it the factor $r - s$ we find a quadratic equation, giving the further integral point $P_d(2d + 3, 6d + 7) = 0$ if $6d + 7$ is a square. Looking at the coefficients of $t^{r+s-\nu}$ for larger values of ν leads to curves of higher degree (in fact, because of a hidden symmetry of $H(t)$, to the same ones as in (VII) above) and therefore to no new infinite families.

(X) $x = 2d - 5$ *or* $2d - 6$. We could also have obtained the solutions (IV) by observing that for $x = 2d - 2\nu - 1$ and $x = 2d - 2\nu - 2$ construction (I) gives all but ν of the roots of $P_d(x, \cdot) = 0$. The case $\nu = 1$ corresponds to (IV), while for $\nu = 2$ we are left with a quadratic polynomial and find

$$6d^2 - 9d + 4 = e^2 \Rightarrow P_d(2d - 5, 5 - 6d \pm 2e) = 0,$$
$$10d^2 - 15d + 9 = f^2 \Rightarrow P_d(2d - 6, 10 - 10d \pm 2f) = 0.$$

The conditions on d are in each case Pell-type equations having infinitely many solutions, the first being $d = 4, 33, 320, 3161, \ldots$ and $d = 8, 33, 144, 637, \ldots$, respectively. Here again, larger ν no longer give infinite families of solutions.

We summarize the above constructions (excluding (X) and the elliptic curves in (VII)) and the numbers of solutions they yield by the table

(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)	(IX)
d^2+d	d	1	2	[odd]	$2\varepsilon_{16d+1}$	$2\varepsilon_{48d+1}$	ε_{2d+2}	ε_{6d+7}

where "[odd]" means 1 if d is odd and 0 otherwise and ε_n denotes 1 if n is a square and 0 otherwise. To get the constructions (VI) and (VII) to work simultaneously we need $16d + 1 = a^2$ and $48d + 1 = b^2$ for some integers a and b, so $3a^2 - b^2 = 2$. This is a Pell-type equation whose positive solutions are given by $(b + a\sqrt{3})^n = (1 + \sqrt{3})(2 + \sqrt{3})^n$ with $n \geq 0$. The common value of $(a^2 - 1)/16$ and $(b^2 - 1)/48$ is then integral if n is congruent to 0 or 3 (mod 4) and odd if n is congruent to 3 or 4 (mod 8), so for n satisfying the latter congruence all seven constructions (I)–(VII) apply and we get $d^2 + 2d + 8$ integral solutions of $P_d(x, y) = 0$. The set of values of d obtained in this way is not very dense (its only elements less than 10^{20} are $d = 105$, 1463, 148772396955, and 2072132179845), but it is still infinite, proving Theorem 2. We can also combine either (V) or (VII) with (VIII) or (IX) instead of with each other to produce other infinite Pell-like families, but this gives (for d odd) only $d^2 + 2d + 7$ rather than $d^2 + 2d + 8$ solutions, and we cannot combine three of these constructions because this corresponds to finding integral points on an elliptic curve over $\mathbb{Q}$ and there are only finitely many.

Remarks. 1. It is very striking that in all of the above constructions except for (IV) and (X) the values of y are perfect squares, and that the same holds for most (all but 3) of the "sporadic" solutions listed in [5]. From a Diophantine point of view, replacing the equation $P_d(x, y) = 0$ by $P_d(x, y^2) = 0$ makes the problem incomparably harder to solve (for instance, already for $d = 2$ the original equation is easy and has infinitely many solutions, while the latter has only finitely many and the problem of finding them is difficult), so that it is downright perverse to throw away the extra information and list the solutions found merely as solutions of the easier problem. The reason that this was nevertheless done in [5] and here is not so much in order to capture the two extra zeros in (IV), but because we are looking for examples of polynomials with many zeros relative to their degree, and replacing y by y^2 in $P_d(x, y)$ doubles the degree. In other words, in general there are fewer and fewer rational or integral points on curves as

the degree (or genus) goes up, but for these special polynomials the opposite is happening and it is therefore advantageous to forget that y is usually a square. Nevertheless, it seemed reasonable to supplement the search described in [5] (which found all solutions with $d \le 12$, $|x| \le 1000$) by a systematic search for integral zeros of $P_d(x, y^2) = 0$. A search for all zeros in the range $d \le 50$, $0 \le y \le 1000$ led to the discoveries of some of the above families and produced the following zeros which do not belong to any of the families (I)–(IX):

$$\begin{aligned}(d, \sqrt{y}, x) = {} & (2,6,66), (2,91,1521), (2,91,15043), (3,5,67), (3,35,345),\\ & (7,4,98), (17,6,514), (18,21,67), (18,55,67), (22,5,67),\\ & (22,5,465), (31,6,66), (31,6,932), (31,11,67), (31,23,67),\\ & (31,94,132), (35,94,132), (42,4,98), (42,4,576), (43,55,177)\end{aligned}$$

with no further discernible patterns.

2. Both in [5] and in the introduction to this paper, the emphasis has been on integral solutions of $P_d(x, y) = 0$ or other polynomial equations in two variables. Actually, there is no real distinction in this context between rational and integral solutions, if we not quantify things by putting some restriction on the heights of the polynomials, because if an equation $P(x, y) = 0$ of degree d has $\ge C$ rational solutions, then the rescaled equation $N^d P(x/N, y/N) = 0$, where N is any common denominator of these solutions, clearly has $\ge C$ integral solutions. For the particular family of polynomials P_d, the large number of integral solutions was so striking that it seemed a pity to throw away this information by replacing "integral" by "rational" in the statement of the theorems, especially as these polynomials have relatively small height and this property would be destroyed by too vigorous a rescaling. Nevertheless, for the sake of completeness and to have a clear conscience we should also look for rational solutions. A small computer search (specifically, a search for all solutions of $P_d(x, a/b) = 0$ or $P_d(x, a^2/b^2) = 0$ with $3 < d \le 12$, $2 \le b \le 20$, and $|a| \le 1000$, the equations $P_2 = 0$ and $P_3 = 0$ with infinitely many solutions being omitted) yielded only one additional family,

(X) $P_d\big(d - \frac{3}{4}, \frac{1}{4}\big) = 0$ for d odd (whose proof by residue calculus we omit), together with the handful of sporadic solutions:

$$\begin{aligned} d = 4: \quad & (x,y) = \big(\tfrac{5}{3}, -\tfrac{1}{3}\big),\ \big(-\tfrac{10}{11}, -\tfrac{76}{11}\big),\ \big(\tfrac{71}{11}, \tfrac{71}{11}\big),\ \big(\tfrac{505}{121}, \tfrac{25}{121}\big),\\ d = 5: \quad & (x,y) = \big(\tfrac{7}{17}, -\tfrac{43}{17}\big),\ \big(-\tfrac{5}{19}, -\tfrac{81}{19}\big),\ \big(\tfrac{124}{19}, \tfrac{124}{19}\big).\end{aligned}$$

Two of these are easy to explain and do not generalize (the polynomial $P_d(x, x)$ vanishes at $x = 0, 1, 4, \ldots, [\sqrt{2d-1}\,]^2$, and for $d = 4$ or 5 this leaves room for only one further root, which must then be rational) and all of them have $d \le 5$, so this data suggests that the special equations $P_d(x, y) = 0$

indeed have almost no non-integral rational solutions. Nevertheless, by using the new family (X) we can present the following minuscule improvement of the previous results:

THEOREM 4. *The equation* $P_d(x/4, y/4) = 0$ *has at least* $d^2 + 2d + 5$ *integral solutions for any odd* d *and at least* $d^2 + 2d + 9$ *integral solutions for infinitely many values of* d.

Acknowledgements. We would like to thank A. Bremner for spotting the extra points (V) discussed in Section 4. The first author would like to thank the NSF, TARP and the Alfred P. Sloan Foundation for financial support. The second author would like to thank the NSA for financial support.

References

[1] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, in: Proc. of the Millennium Conference, Urbana, 2000, to appear.
[2] A. Bremner, Math. Rev. 2000b:14025.
[3] L. Caporaso, *Counting rational points on algebraic curves*, in: Number Theory, I (Rome, 1995), Rend. Sem. Mat. Univ. Politec. Torino 53 (1995), 223–229.
[4] N. Elkies, *Curves with many points*, preprint available at http://www.math.harvard.edu/~elkies/misc.html.
[5] F. Rodríguez Villegas and J. F. Voloch, *On certain plane curves with many integral points*, Experiment. Math. 8 (1999), 57–62.
[6] W. Ruppert, *Solving algebraic equations in roots of unity*, J. Reine Angew. Math. 435 (1993), 119–156.
[7] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52 (1986), 1–19.

Department of Mathematics
University of Texas
Austin, TX 78712, U.S.A.
E-mail: villegas@math.utexas.edu
voloch@math.utexas.edu

Max-Planck-Institut für Mathematik
D-53111 Bonn, Germany
E-mail: zagier@mpim-bonn.mpg.de

Received on 10.7.2000 (3850)