Journal of Number Theory **77**, 62–70 (1999)
Article ID jnth.1999.2381, available online at http://www.idealibrary.com on IDEAL®

Reducibility of Polynomials $f(x, y)$ Modulo p

Wolfgang M. Ruppert

Mathematisches Institut, Universität Erlangen-Nürnberg, Bismarckstrasse $1\frac{1}{2}$, D-91054 Erlangen, Germany
E-mail: ruppert@mi.uni-erlangen.de

Communicated by M. Pohst

Received October 10, 1998

We consider absolutely irreducible polynomials $f \in \mathbf{Z}[x, y]$ with $\deg_x f = m$, $\deg_y f = n$ and height H. We show that for any prime p with $p > [m(n+1)\, n^2 +$ ... are infinitely many absolutely irreducible polynomials $f \in \mathbf{Z}[x, y]$ which are reducible mod p where p is a prime with $p \geqslant H^{2m}$.

1. INTRODUCTION

It is well known that for an absolutely irreducible polynomial $f \in \mathbf{Z}[x, y]$ the reduction $f \bmod p$ is also absolutely irreducible if the prime p is large enough. For small p the polynomial $f \bmod p$ may be reducible, e.g., $f = x^9 y - 9x^9 - 2x + 9y + 2$ is absolutely irreducible over $\mathbf{Q}$ but reducible modulo $p = 18694025526754501\!1$ where $x - 93470127633772547$ divides $f \bmod p$. It is natural to ask how large p has to be to be sure that $f \bmod p$ is absolutely irreducible. In [R1] we showed that

$$p > d^{3d^2-3} \cdot H(f)^{d^2-1}$$

is sufficient for absolute irreducibility mod p where d is the total degree of f and $H(f)$ the height[1] of f. Sometimes it is more natural to consider the polynomial having degree m in x and n in y. For this case Zannier [Z] has shown that

$$p > e^{12n^2m^2} (4n^2 m)^{8n^2 m} \cdot H(f)^{2(2n-1)^2 m}$$

[1] The height of a polynomial $f = \sum_{i,j} a_{ij} x^i y^j \in \mathbf{Z}[x, y]$ as we use it is defined by $H(f) = \max_{i,j} |a_{ij}|$.

0022-314X/99 $30.00

is sufficient for absolute irreducibility mod p. Our aim is to improve Zannier's estimate by showing the following theorem:

THEOREM. *Let $f \in \mathbf{Z}[x, y]$ be an absolutely irreducible polynomial with degree $m \geqslant 1$ in x, $n \geqslant 1$ in y and height $H(f)$. If p is a prime with*

$$p > [m(n+1)\, n^2 + (m+1)(n-1)\, m^2]^{mn + (n-1)/2} \cdot H(f)^{2mn + n - 1}$$

then the reduced polynomial f mod p is also absolutely irreducible.

The basic ingredient of the proof is the structure theorem for closed 1-forms as it was already used in [R1]. In Section 2 the connection between closed 1-forms and reducibility is given in two lemmas and applied to prove the theorem. The lemmas are proved in Section 3.

To test the quality of the estimate in the theorem we construct examples of polynomials $f \in \mathbf{Z}[x, y]$ in Section 4 with a certain reducibility behavior. Assuming the Bouniakowsky conjecture (which will also be explained in Section 4) one gets the following result:

PROPOSITION. *Let $m, n > 1$ be integers. If the Bouniakowsky conjecture is true there are infinitely many polynomials $f \in \mathbf{Z}[x, y]$ with $\deg_x f = m$ and $\deg_y f = n$ which are absolutely irreducible over $\mathbf{Q}$ but reducible for a prime p with*

$$p \geqslant H(f)^{2m}.$$

In case $n = 1$ the inequality in the theorem is $p > (2m)^m$. $H(f)^{2m}$. The proposition shows then that the exponent $2m$ is best possible. In case $n = 2$ the exponent in the theorem is $4m + 1$. In [R2] it is shown that the exponent can be improved to 6 (for $m = 2$), $6\frac{2}{3}$ (for $m = 3$) and $2m$ (for $m \geqslant 4$). This supports my belief that the best exponent in the theorem will be smaller than $2mn + n - 1$ if $n \geqslant 2$.

2. A CRITERION FOR REDUCIBILITY

If $f(x, y)$ is a polynomial with $\deg_x f = m$ and $\deg_y f = n$ we write $\deg f = (m, n)$. The notation $\deg f \leqslant (m, n)$ will mean that $\deg_x f \leqslant m$, $\deg_y f \leqslant n$. If it happens that we write $\deg f \leqslant (m, n)$ with $m < 0$ or $n < 0$ then $f = 0$.

The following lemmas contain our criterion for reducibility.

LEMMA 1. *Let k be an arbitrary algebraically closed field and $f(x, y) \in k[x, y]$ a reducible polynomial with* $\deg f = (m, n)$. *Then there are polynomials $r, s \in k[x, y]$ with* $\deg r \leqslant (m-1, n)$ *and* $\deg s \leqslant (m, n-2)$ *such that*

$$\frac{\partial}{\partial y}\left(\frac{r}{f}\right) = \frac{\partial}{\partial x}\left(\frac{s}{f}\right) \qquad \textit{and} \qquad (r, s) \neq (0, 0).$$

LEMMA 2. *Let k be an arbitrary algebraically closed field of characteristic* 0 *and $f(x, y) \in k[x, y]$ with* $\deg f = (m, n)$ *and* $n \geqslant 1$. *If there are polynomials $r, s \in k[x, y]$ with* $\deg r \leqslant (m-1, n)$ *and* $\deg s \leqslant (m, n-2)$ *such that*

$$\frac{\partial}{\partial y}\left(\frac{r}{f}\right) = \frac{\partial}{\partial x}\left(\frac{s}{f}\right) \qquad \textit{and} \qquad (r, s) \neq (0, 0)$$

then f is reducible.

The proof of the lemmas will be postponed to the next section. We remark that the example $f = x$, $r = 1$, $s = 0$ shows that $n \geqslant 1$ is a necessary condition in Lemma 2.

We reformulate the lemmas: Let $f \in k[x, y]$ have degree (m, n) and assume that $m, n \geqslant 1$. When do we find $r, s \in k[x, y]$ with $\deg r \leqslant (m-1, n)$ and $\deg s \leqslant (m, n-2)$ such that the equation

$$\frac{\partial}{\partial y}\left(\frac{r}{f}\right) = \frac{\partial}{\partial x}\left(\frac{r}{f}\right) \tag{1}$$

holds? We write

$$f = \sum_{\substack{0 \leqslant i \leqslant m \\ 0 \leqslant j \leqslant n}} a_{ij} x^i y^j, \qquad r = \sum_{\substack{0 \leqslant i \leqslant m-1 \\ 0 \leqslant j \leqslant n}} u_{ij} x^i y^j, \qquad s = \sum_{\substack{0 \leqslant i \leqslant m \\ 0 \leqslant j \leqslant n-2}} v_{ij} x^i y^j$$

with unknowns u_{ij} $(0 \leqslant i \leqslant m-1,\ 0 \leqslant j \leqslant n)$ and v_{ij} $(0 \leqslant i \leqslant m,\ 0 \leqslant j \leqslant n-2)$. (There are $m(n+1) + (m+1)(n-1) = 2mn + n - 1$ unknowns u_{ij} and v_{ij} if $m, n \geqslant 1$.) Equation (1) can be written as

$$\frac{\partial r}{\partial y} f - r \frac{\partial f}{\partial y} - \frac{\partial s}{\partial x} f + s \frac{\partial f}{\partial x} = 0.$$

We have

$$\frac{\partial r}{\partial y} f - r \frac{\partial f}{\partial y} - \frac{\partial s}{\partial x} f + s \frac{\partial f}{\partial x} = \sum_{k, l} g_{kl} x^k y^l$$

with

$$g_{kl} = \sum_{(i,j)\in A_{kl}} (-l+2j-1)\, a_{k-i,\, l-j+1} u_{ij} + \sum_{(i,j)\in B_{kl}} (k-2i+1)\, a_{k-i+1,\, l-j} v_{ij},$$

where

$$A_{kl} = \{(i,j) : 0 \leqslant k-i \leqslant m,\ 0 \leqslant l-j+1 \leqslant n,\ 0 \leqslant i \leqslant m-1,\ 0 \leqslant j \leqslant n\},$$
$$B_{kl} = \{(i,j) : 0 \leqslant k-i+1 \leqslant m,\ 0 \leqslant l-j \leqslant n,\ 0 \leqslant i \leqslant m,\ 0 \leqslant j \leqslant n-2\}.$$

One sees that $\deg \sum g_{kl} x^k y^l \leqslant (2m-1, 2n-2)$. Equation (1) is satisfied iff we find $u_{ij}, v_{ij} \in k$ with

$$g_{00} = \cdots = g_{2m-1,\, 2n-2} = 0.$$

We can write this as a matrix equation

$$\begin{pmatrix} g_{00} \\ \vdots \\ g_{2m-1,\, 2n-2} \end{pmatrix} = M(f) \cdot \begin{pmatrix} u_{00} \\ \vdots \\ u_{m-1,\, n} \\ v_{00} \\ \vdots \\ v_{m,\, n-2} \end{pmatrix} = 0,$$

where the entries of the matrix $M(f)$ are coefficients of certain g_{kl} with respect to u_{ij} and v_{ij}. With these notations it is clear that equation (1) has a nontrivial solution iff $M(f)$ has rank $< (2mn+n-1)$, i.e. all $(2mn+n-1) \times (2mn+n-1)$-submatrices of $M(f)$ vanish. Now we can reformulate the two lemmas for $f \in k[x, y]$ in terms of the matrix $M(f)$:

- If f is reducible then rank $M(f) < 2mn+n-1$.
- If k has characteristic 0 and rank $M(f) < 2mn+n-1$ then f is reducible.

We apply this to prove the theorem: Let $f \in \mathbf{Z}[x, y]$ be absolutely irreducible of degree (m, n). Then the matrix $M(f)$ has rank $2mn+n-1$, i.e., there is a $(2mn+n-1) \times (2mn+n-1)$-submatrix M_0 of $M(f)$ with $\det M_0 \neq 0$. We will estimate $|\det M_0|$ using Hadamard's estimate for determinants. To do this we have to know the L_2-norm of the rows of M_0. A row of M_0 is given by the coefficients of a linear form g_{kl} with respect to the variables u_{ij} and v_{ij}. We have

$$\begin{aligned} \|g_{kl}\|_2^2 &= \sum_{(i,j)\in A_{kl}} (-l+2j-1)^2\, a_{k-i,\, l-j+1}^2 + \sum_{(i,j)\in B_{k_l}} (k-2i+1)^2\, a_{k-i+1,\, l-j}^2 \\ &\leqslant \left(\sum_{(i,j)\in A_{kl}} (-l+2j-1)^2 + \sum_{(i,j)\in B_{kl}} (k-2i+1)^2 \right) \cdot H(f)^2. \end{aligned}$$

If $(i, j) \in A_{kl}$ then $0 \leqslant l-j+1 \leqslant n$ and $0 \leqslant j \leqslant n$ so that $-n \leqslant -(l-j+1)+j \leqslant n$ and $(-l+2j-1)^2 \leqslant n^2$. Furthermore $\# A_{kl} \leqslant m(n+1)$.

If $(i, j) \in B_{kl}$ then $0 \leqslant k-i+1 \leqslant m$ and $0 \leqslant i \leqslant m$ so that $-m \leqslant (k-i+1) - i \leqslant m$ and $(k-2i+1)^2 \leqslant m^2$. Furthermore $\# B_{kl} \leqslant (m+1)(n-1)$.

This implies

$$\begin{aligned} \|g_{kl}\|_2^2 &\leqslant (n^2 \cdot \# A_{kl} + m^2 \cdot \# B_{kl}) \cdot H(f)^2 \\ &\leqslant [m(n+1)n^2 + (m+1)(n-1)m^2] \cdot H(f)^2 \end{aligned}$$

so that the L_2-norm of a row of M_0 is

$$\leqslant \sqrt{[m(n+1)n^2 + (m+1)(n-1)m^2] \cdot H(f)^2}$$

and therefore using Hadamard

$$\begin{aligned} |\det M_0| &\leqslant \sqrt{[m(n+1)n^2 + (m+1)(n-1)m^2] \cdot H(f)^2}^{\,2mn+n-1} \\ &= [m(n+1)\, n^2 + (m+1)(n-1)\, m^2]^{mn+(n-1)/2} \cdot H(f)^{2mn+n-1}. \end{aligned}$$

Now if p is any prime with

$$p > [m(n+1)\, n^2 + (m+1)(n-1) m^2]^{mn+(n-1)/2} \cdot H(f)^{2mn+n-1}$$

then $0 < |\det M_0| < p$ which implies that $\det M_0 \not\equiv 0 \bmod p$ so that $M(f)$ considered as a matrix over $\mathbf{F}_p$ has rank $2mn+n-1$ and $f \bmod p$ is absolutely irreducible by the above criterion. This proves our theorem.

3. PROOF OF LEMMAS 1 AND 2

We start with a remark: If k is an algebraically closed field and $g \in k[x, y]$ satisfies $\partial g/\partial x = \partial g/\partial y = 0$ then g is constant in characteristic 0 or a p-power in characteristic p. In each case, g is not irreducible.

Proof of Lemma 1. Let $f \in k[x, y]$ be reducible of degree (m, n). We have to construct a nontrivial solution for the equation $(\partial/\partial y)(r/f) = (\partial/\partial x)(s/f)$ with $\deg r \leqslant (m-1, n)$ and $\deg s \leqslant (m, n-2)$. We distinguish different cases:

Case I. f is squarefree. We write $f = gh$ with $\deg_y g = l$ and we can assume that h is irreducible. Writing

$$\begin{aligned} g &= b_0(x) + b_1(x)\, y + \cdots + b_l(x)\, y^l, \\ h &= c_0(x) + c_1(x)\, y + \cdots + c_{n-l}(x)\, y^{n-l} \end{aligned}$$

gives

$$\frac{\partial g}{\partial y} h = b_1(x)\, c_0(x) + \cdots + l b_l(x)\, c_{n-l}(x)\, y^{n-1},$$

$$g \frac{\partial h}{\partial y} = b_0(x)\, c_1(x) + \cdots + (n-l)\, b_l(x)\, c_{n-l}(x)\, y^{n-1}.$$

Case I.1. $l \neq 0$ in k. Take

$$r = (n-l) \frac{\partial g}{\partial x} h - lg \frac{\partial h}{\partial x} \qquad \text{and} \qquad s = (n-l) \frac{\partial g}{\partial y} h - lg \frac{\partial h}{\partial y}.$$

One sees at once that $(\partial/\partial y)(r/f) = (\partial/\partial x)(s/f)$ holds and that by construction $\deg r \leqslant (m-1, n)$, $\deg s \leqslant (m, n-2)$. If we had $r = s = 0$ then h would divide $\partial h/\partial x$ and $\partial h/\partial y$ which would imply $\partial h/\partial x = \partial h/\partial y = 0$, contradicting the irreducibility of h. Therefore $(r, s) \neq (0, 0)$ and we are done.

Case I.2. $l = 0$ in k. Then $\deg_y (\partial g/\partial y)\, h \leqslant n-2$. Take

$$r = \frac{\partial g}{\partial x} h, \qquad s = \frac{\partial g}{\partial y} h.$$

Then the equation $(\partial/\partial y)(r/f) = (\partial/\partial x)(s/f)$ is satisfied with $\deg r \leqslant (m-1, n)$ and $\deg s \leqslant (m, n-2)$. Also $(r, s) \neq (0, 0)$ else g would be a p-power contradicting the fact that f is supposed to be squarefree.

Case II. f is not squarefree. We write $f = g^2 h$ and we can assume that g is irreducible. Take

$$r = h \frac{\partial g}{\partial x} \qquad \text{and} \qquad s = h \frac{\partial g}{\partial y}.$$

Then $(r, s) \neq (0, 0)$ because g is irreducible and

$$\frac{r}{f} = \frac{1}{g^2} \frac{\partial g}{\partial x} = \frac{\partial}{\partial x}\left(-\frac{1}{g}\right), \qquad \frac{s}{f} = \frac{1}{g^2} \frac{\partial g}{\partial y} = \frac{\partial}{\partial y}\left(-\frac{1}{g}\right)$$

shows that $(\partial/\partial y)(r/f) = (\partial/\partial x)(s/f)$ holds. It is clear that $\deg r \leqslant (m-1, n)$ and $\deg s \leqslant (m, n-2)$. ∎

Proof of Lemma 2. Suppose that k is algebraically closed of characteristic 0, $f \in k[x, y]$ is irreducible with $\deg f = (m, n)$, and

$$\frac{\partial}{\partial y}\left(\frac{r}{f}\right) = \frac{\partial}{\partial x}\left(\frac{s}{f}\right)$$

with $\deg r \leqslant (m-1, n)$, $\deg s \leqslant (m, n-2)$, and $(r, s) \neq (0, 0)$. The equation implies that

$$\omega = \frac{r}{f}\, dx + \frac{s}{f}\, dy$$

is a nontrivial closed differential form. Now the structure theorem for closed 1-forms (cf. [R1, Satz 2, p. 172]) says that ω has the form

$$\omega = \sum_{i=1}^{u} \lambda_i \frac{dp_i}{p_i} + d\left(\frac{g}{q_1^{e_1} \cdots q_v^{e_v}}\right),$$

where $p_i, q_j \in k[x, y]$ are irreducible, $g \in k[x, y]$, $\lambda_i \in k$, $e_j \geqslant 0$, $p_1, ..., p_u$ are pairwise prime, $q_1, ..., q_v, g$ are pairwise prime. Comparing the coefficients of dx and dy gives

$$\frac{r}{f} = \frac{\lambda_1(\partial p_1/\partial x)}{p_1} + \cdots + \frac{\lambda_r(\partial p_u/\partial x)}{p_u} + \frac{\partial g/\partial x}{q_1^{e_1} \cdots q_v^{e_v}} - \frac{e_1\, g(\partial q_1/\partial x)}{q_1^{e_1+1} q_2^{e_2} \cdots q_v^{e_v}}$$
$$- \cdots - \frac{e_v\, g(\partial q_v/\partial x)}{q_1^{e_1} \cdots q_{v-1}^{e_{v-1}} q_v^{e_v+1}}$$

$$\frac{s}{f} = \frac{\lambda_1(\partial p_1/\partial y)}{p_1} + \cdots + \frac{\lambda_u(\partial p_u/\partial y)}{p_u} + \frac{\partial g/\partial y}{q_1^{e_1} \cdots q_v^{e_v}} - \frac{e_1\, g(\partial q_1/\partial y)}{q_1^{e_1+1} q_2^{e_2} \cdots q_v^{e_v}}$$
$$- \cdots - \frac{e_v\, g(\partial q_v/\partial y)}{q_1^{e_1} \cdots q_{v-1}^{e_{v-1}} q_v^{e_v+1}}.$$

$k[x, y]$ is factorial and therefore we have for each p_i and q_j a valuation v_{p_i} and v_{q_j}.

If $g \neq 0$ and $e_j \geqslant 1$ for some j we would get $v_{q_j}(r/f) = -e_j - 1 \leqslant -2$ or $v_{q_j}(s/f) = -e_j - 1 \leqslant -2$ as $(\partial q_j/\partial x, \partial q_j/\partial y) \neq (0, 0)$, a contradiction to the irreducibility of f. Therefore we can assume $e_1 = \cdots = e_v = 0$. If $\lambda_i \neq 0$ and p_i is prime to f then $(\partial p_i/\partial x, \partial p_i/\partial y) \neq (0, 0)$ would imply $v_{p_i}(r/f) = -1$ or $v_{p_i}(s/f) = -1$, a contradiction. We can write now

$$\omega = \lambda \frac{df}{f} + dg$$

with $\lambda \in k$ which gives

$$r = \lambda \frac{\partial f}{\partial x} + f \frac{\partial g}{\partial x} \qquad \text{and} \qquad s = \lambda \frac{\partial f}{\partial y} + f \frac{\partial g}{\partial y}.$$

If $\partial g/\partial x \neq 0$ then r would have degree $\geqslant m$ in x, a contradiction, if $\partial g/\partial y \neq 0$ then s would have degree $\geqslant n$ in y, a contradiction. Therefore we get

$$r = \lambda \frac{\partial f}{\partial x} \quad \text{and} \quad s = \lambda \frac{\partial f}{\partial y}$$

with $\lambda \neq 0$. As $n \geqslant 1$ we can write $f = a_0(x) + \cdots + a_n(x)\, y^n$ with $a_n(x) \neq 0$ and get $\partial f/\partial y = a_1(x) + \cdots + n a_n(x)\, y^{n-1}$ which shows that s has degree $n-1$ in y, a contradiction. Therefore f cannot be irreducible. This proves the lemma. ∎

4. EXAMPLES

In the following lemma families of polynomials are constructed with an explicit reducibility condition.

LEMMA 3. (1) *Let k be an algebraically closed field of characteristic $\neq 2$, $m, n \geqslant 1$ integers and $t \in k$. The polynomial $f_t(x, y) = (tx^m - 2x + 2) + (x^m - t)\, y^n \in k[x, y]$ is reducible if and only if $(t^2+2)^m - 2^m t = 0$. In this case the factor $x - (t^2+2)/2$ splits off.*

(2) *The polynomial $g_m(t) = (t^2+2)^m - 2^m t \in \mathbf{Z}[t]$ is irreducible over $\mathbf{Q}$ and* $\gcd\{ g_m(l) : l \in \mathbf{N}\} = 1$.

Proof. (1) Suppose first that $tx^m - 2x + 2$ and $x^m - t$ are relatively prime and f_t is reducible. Then f_t is reducible as a polynomial in y with coefficients in $k(x)$ and therefore $(-tx^m + 2x - 2)/(x^m - t)$ is a nontrivial power in $k(x)$. Then $-tx^m + 2x + 2$ and $x^m - t$ have to be nontrivial powers in $k[x]$ and therefore inseparable. But $x^m - t$ is inseparable only if $m = 0$ or $t = 0$ in k and for both cases $-tx^m + 2x - 2$ is separable. So this case cannot happen.

If $tx^m - 2x + 2$ and $x^m - t$ have a common factor $x - u$ for some $u \in k$ then f_t is clearly reducible. This happens iff $tu^m - 2u + 2 = u^m - t = 0$ which is equivalent to $u = (t^2+2)/2$ and $(t^2+2)^m - 2^m t = 0$ which proves part (1) of the lemma.

(2) Let $\alpha \in \bar{\mathbf{Q}}$ be any root of g_m over $\mathbf{Q}$, i.e. $\alpha = ((\alpha^2+2)/2)^m$. Define $\beta = (\alpha^2+2)/2 \in \mathbf{Q}(\alpha)$. Then $\alpha = \beta^m \in \mathbf{Q}(\beta)$ and therefore $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$. Finally $0 = \alpha^2 + 2 - 2\beta = \beta^{2m} - 2\beta + 2$ shows that β is a root of the irreducible Eisenstein polynomial $t^{2m} - 2t + 2$, which implies that $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$ has degree $2m$ over $\mathbf{Q}$. Therefore $g_m = (t^2+2)^m - 2^m t$ is irreducible over $\mathbf{Q}$. From $g_m(0) = 2^m$ and $g_m(1) \equiv 1 \bmod 2$ one sees that $\gcd\{ g_m(l) \colon l \in \mathbf{N}\} = 1$. ∎

To construct infinitely many examples with the right reduction behavior we use the very plausible Bouniakowsky conjecture which was generalized by Schinzel as hypothesis H (cf. [B, S]):

Conjecture (Bouniakowsky). *If* $g(t) \in \mathbf{Z}[t]$ is irreducible and $N = \gcd\{g(l): l \in \mathbf{N}\}$ then there are infinitely many $l \in \mathbf{N}$ such that $(1/N)\,|g(l)|$ is a prime.

Now we prove our proposition of Section 1. We use the notations and results of the previous lemma. Let $m, n \geqslant 1$ be integers and take

$$f_l(x, y) = (lx^m - 2x + 2) + (x^m - l)\, y^n \in \mathbf{Z}[x, y]$$

with $l \in \mathbf{Z}$, $l \geqslant 2$. Then $H(f_l) = l$. As $g_m(l) \neq 0$ in $\mathbf{Q}$ the polynomial f_l is absolutely irreducible over $\mathbf{Q}$. If $p_l = g_m(l)$ is a prime, then $g_m(l) \equiv 0 \bmod p_l$ and $f_l \bmod p_l$ is reducible and

$$p_l = g_m(l) \geqslant l^{2m} = H(f_l)^{2m}.$$

Now the Bouniakowsky conjecture says that there are infinitely many l such that $g_m(l)$ is prime. This proves the proposition.

REFERENCES

[B] V. Bouniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, *Mém. Acad. Sci. St. Pétersbourg (6) Sci. Math. Phys.* **6** (1857), 305–329.

[R1] W. Ruppert, Reduzibilität ebener Kurven, *J. Reine Angew. Math.* **369** (1986), 167–191.

[R2] W. Ruppert, Reducibility of polynomials $a_0(x) + a_1(x)\, y + a_2(x)\, y^2$ modulo p, *Arch. Math.* **72** (1999), 47–55.

[S] A. Schinzel and W. Sierpinski, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; corrig., *Acta Arith.* **5** (1959), 259.

[Z] U. Zannier, On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$, *Arch. Math.* **68** (1997), 129–138.