COLLOQUIUM MATHEMATICUM

VOL. 93 2002 NO. 1

ON PRIME VALUES OF REDUCIBLE QUADRATIC POLYNOMIALS

BY

W. NARKIEWICZ and T. PEZDA (Wrocław)

Abstract. It is shown that Dickson's Conjecture about primes in linear polynomials implies that if f is a reducible quadratic polynomial with integral coefficients and non-zero discriminant then for every r there exists an integer N_r such that the polynomial $f(X)/N_r$ represents at least r distinct primes.

1. It is not difficult to find reducible quadratic polynomials with rational coefficients which can represent prime numbers at integral arguments. E.g. the polynomial $x(x+1)/180180$ represents eight distinct primes attained at $x = 4004$, 5004, 16 379, 25 739, 36 035, 45 044, 180 179 and 180 180.

It has been observed by Y. G. Chen and I. Z. Ruzsa ([1]) that Dickson's Conjecture about primes in linear polynomials implies that for every natural r there exist integers a and N such that the polynomial $X(X+a)/N$ represents at least r primes at integral arguments. Recall that Dickson's Conjecture (see [2]) states that if for positive integers $a_1, \ldots, a_n$ and integers $b_1, \ldots, b_n$ the polynomial $(a_1X + b_1)\ldots(a_nX + b_n)$ does not have a constant prime divisor then there exist infinitely many integers x such that $a_ix + b_i$ is prime for $i = 1, \ldots, n$.

We shall prove that the same is true for any reducible quadratic polynomial f of non-vanishing discriminant. Our proof provides a method for constructing an integer $N = N_r$ such that $f(X)/N_r$ represents r primes, which would be effective, if there were an effective algorithm for constructing primes satisfying Dickson's Conjecture. Unfortunately this method cannot be regarded as very efficient, because already in the simplest case, when $f(X) = X(X+1)$ and $r = 9$, it leads to congruences with moduli having more than 100 digits.

It would be interesting to know whether an analogous assertion can be obtained for reducible polynomials of higher degrees.

2. THEOREM. *Assume the truth of Dickson's Conjecture. If $f(X) = (aX+b)(cX+d)$ is a polynomial with rational integral coefficients, sat-*

2000 *Mathematics Subject Classification*: Primary 11N32; Secondary 11A41.

isfying $a, c > 0$ and $\Delta = ad - bc \neq 0$, then for every natural r there exists an integer N such that $f(X)/N$ represents at least r distinct primes.

Proof. Fix $r > |a|, |b|, |c|, |d|, |\Delta|$. Clearly without loss of generality we may assume $(a, b) = 1$. Let q be a prime such that $q \equiv b \pmod a$ and $q > r!c|\Delta|$. Choose r primes, say $x_1 = q < x_2 < \ldots < x_r$, congruent to q mod $cr!$ and denote by P_r the product of all primes not exceeding r. Moreover put $D = \prod_{j=1}^r x_j^2$ and $D_i = D/x_i^2$ $(i = 1, \ldots, r)$.

LEMMA 1. *If $\Delta, x_i, a, b, c, d, r$ are as above then the system of congruences*

$$\begin{aligned} \lambda &\equiv \Delta x_i + c x_i^2 && \pmod{cP_r x_i^2} && (i = 1, \ldots, r), \\ \lambda &\equiv a d x_i && \pmod{ac} && (i = 1, \ldots, r) \end{aligned}$$

is solvable.

Proof. As for $1 \leq i \neq j \leq r$ we have

$$(cP_r x_i^2, cP_r x_j^2) = cP_r \quad \text{and} \quad (ac, cP_r x_i^2) \mid ac,$$

the above system of congruences is solvable if the following conditions are satisfied for $1 \leq i, j \leq r$:

$$\begin{aligned} \Delta x_i + c x_i^2 &\equiv \Delta x_j + c x_j^2 && \pmod{cP_r}, \\ a d x_i &\equiv a d x_j && \pmod{ac}, \\ \Delta x_i + c x_i^2 &\equiv a d x_j && \pmod{ac}. \end{aligned}$$

(We use here a version of the Chinese Remainder Theorem which rarely occurs in textbooks, but may be found e.g. in [3], Vol. I, p. 279.)

The first two conditions hold because $cP_r \mid x_i - x_j$ and $ac \mid a(x_i - x_j)$ and the third is equivalent to $ac \mid ad(x_i - x_j) + c x_i (x_i - b)$ and thus it suffices to observe that $c \mid x_i - x_j$ and $a \mid x_i - b$. ■

LEMMA 2. *Let λ be a positive solution of the system of congruences occurring in Lemma 1, let x_i, c, a, d, b, r be as above and put*

$$\alpha_i = a D_i, \qquad \beta_i = \frac{\lambda - \Delta x_i}{c x_i^2} \qquad (i = 1, \ldots, r).$$

Then the product $G(X)$ of the linear polynomials

$$\Phi_i(X) = \alpha_i X + \beta_i \quad (i = 1, \ldots, r)$$

does not have a constant prime divisor.

Proof. Assume that p is a prime dividing $G(n)$ for all integers n. Assume first $p > r$. In this case one of the factors of G, say Φ_i, must have all its coefficients divisible by p. Indeed, otherwise the polynomial $\widehat{G}(X) = G(X) \bmod p \in \mathbb{F}_p(X)$ would have more than $\deg \widehat{G}(X)$ roots in the field $\mathbb{F}_p$ of p elements, which is not possible.

Because $(a,p)=1$ we now get $p\,|\,D_i$ and thus $p=x_k$ for some $k\neq i$. Moreover x_k does not divide c and this implies $x_k\,|\,\lambda-\Delta x_i$. Taking into account the congruence

$$\lambda\equiv\Delta x_k+cx_k^2 \pmod{x_k^2}$$

we get $x_k\,|\,\lambda$. Finally we arrive at $x_k\,|\,\lambda-(\lambda-\Delta x_i)=\Delta x_i$ and thus $x_k\,|\,\Delta$, which contradicts $x_k\geq q>|\Delta|$.

Hence we must have $p\leq r$. In view of $p\,|\,G(0)$ we have $p\,|\,(\lambda-\Delta x_i)/cx_i^2$ for some i, but

$$\frac{\lambda-\Delta x_i}{cx_i^2}\equiv 1 \pmod{P_r}$$

hence the same congruence also holds mod p, a contradiction. ■

Dickson's Conjecture implies the existence of infinitely many integers T such that the numbers $p_i=\alpha_iT+\beta_i$ are prime for $i=1,\ldots,r$. As the numbers α_i are different the primes p_i would be pairwise distinct if we choose T sufficiently large.

Now observe that

$$p_ix_i=aD_iTx_i+\frac{\lambda-\Delta x_i}{cx_i}\equiv\frac{\lambda-\Delta x_i}{cx_i}\equiv\frac{\lambda-adx_i}{cx_i}+b \pmod{a},$$

and since ac and x_i are coprime and both divide $\lambda-adx_i$, it follows that $acx_i\,|\,\lambda-adx_i$. This shows that the numbers

$$s_i=\frac{p_ix_i-b}{a}$$

are integers.

Finally put

$$N=cDT+\frac{\lambda}{a}$$

and observe that

$$f(s_i)=(as_i+b)(cs_i+d)=p_iN,$$

thus $F(s_i)/N=p_i$ for $i=1,\ldots,r$, as asserted. ■

Corollary. *If Dickson's Conjecture is true, then for every r there exist r distinct primes $p_1,\ldots,p_r$ such that the system of quadratic equations*

$$p_iy_j^2-p_jy_i^2=p_i-p_j \quad (1\leq i<j\leq r) \tag{1}$$

is solvable in odd integers $y_i\neq\pm1$.

Proof. Applying the theorem in the case $f(X)=X(X+1)$ we get the existence of primes $p_1,\ldots,p_r$ and integers $x_1,\ldots,x_r$ distinct from 0 and -1 such that

$$p_ix_j(x_j+1)=p_jx_i(x_i+1),$$

hence the numbers $y_j=2x_j+1$ satisfy (1). ■

3. A simple computation with PARI shows that for N in the interval $[1, 12 \cdot 10^6]$ the polynomial $x(x+1)/N$ does not represent more than eight distinct primes, eight primes occurring only once, for $N = 180\,180$. For eleven N's of that interval, namely for $N = 2310$, 6090, 8970, 229 710, 787 710, 1 841 070, 3 254 790, 4 857 090, 5 199 810, 7 414 890 and 7 591 290 one gets seven primes. Observe that for eight N's of this list the numbers $N \pm 1$ form a pair of twin primes. Moreover for 114 numbers $N \leq 12 \cdot 10^6$ six primes are represented.

REFERENCES

[1] Y. G. Chen and I. Z. Ruzsa, *Prime values of reducible polynomials*, *I*, Acta Arith. 95 (2000), 185–193.

[2] L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. (2) 33 (1904), 155–161.

[3] O. Zariski and P. Samuel, *Commutative Algebra*, Springer 1974.

Institute of Mathematics
Wrocław University
Plac Grunwaldzki 2/4
50-384 Wrocław, Poland
E-mail: narkiew@math.uni.wroc.pl
pezda@math.uni.wroc.pl

Received 4 December 2001;
revised 7 March 2002 (4142)