Записки научных
семинаров ПОМИ
Том 429, 2014 г.

A. N. Andrianov

ON PRIME VALUES OF SOME QUADRATIC POLYNOMIALS

The problem on prime values of polynomials in one variable with rational integral coefficients is solved up to now only for the polynomials of degree one by famous Dirichlet theorem on prime numbers in arithmetical progressions. In this paper we start to study properties of prime numbers represented by certain polynomials of degree two.

§1. Sums of two squares

We shall prove here the following theorem.

Theorem 1. *Let p be a prime number, $p \equiv 1 \pmod 4$, and let $p = A^2+B^2$ be a representation of p as sum of two integral squares with even A and odd B. Then the following congruences are fulfilled:*

$$\begin{aligned} 4A^2\left(\left(\frac{p-1}{4}\right)!\right)^4 &\equiv 1 \pmod p,\\ 4B^2\left(\left(\frac{p-1}{4}\right)!\right)^4 &\equiv -1 \pmod p. \end{aligned} \tag{1.1}$$

Corollary. *A prime number p, $p \equiv 1 \pmod 4$, has the form A^2+1 with integral A if and only if it satisfies the congruence*

$$4\left(\left(\frac{p-1}{4}\right)!\right)^4 \equiv -1 \pmod p. \tag{1.2}$$

Proof. For a prime number p, $p \equiv 1 \pmod 4$, and an integer K let us consider the sum of Legendre symbols of the form

$$S(K) = \sum_{x=0}^{p-1}\left(\frac{x(x^2+K)}{p}\right). \tag{1.3}$$

Lemma 1 (D. S. Gorshkov). *The numbers $S(K)$ are always even, for integral t the sums satisfy the relations $S(Kt^2) = \left(\frac{t}{p}\right)S(K)$, where $\left(\frac{t}{p}\right)$*

Key words and phrases: quadratic polynomials, sums of squares.

is the Legendre symbol, and the following expansion is correct

$$p=\left(\frac{1}{2}S(1)\right)^2+\left(\frac{1}{2}S(L)\right)^2 \quad \textit{with} \quad \left(\frac{L}{p}\right)=-1. \tag{1.4}$$

Proof. The proof (compare [2], Chap. 5). The sums $S(K)$ are even, since the summands with $x=x_1$ and $x=-x_1$ are equal. Further, we have

$$S(Kt^2)=\sum_{x=0}^{p-1}\left(\frac{xt(x^2t^2+Kt^2)}{p}\right)=\left(\frac{t}{p}\right)S(K).$$

Finally, if we set $p-1=2d$, then we obtain

$$d(S(1))^2+d(S(L))^2=\sum_{t=1}^{d}(S(t^2))^2+\sum_{t=1}^{d}(S(Lt^2))^2$$
$$=\sum_{K=0}^{p-1}(S(K))^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{K=0}^{p-1}\left(\frac{xy(x^2+K)(y^2+K)}{p}\right),$$

where, when y is not equal to x or $p-x$, the summation on K will give $-\left(\frac{xy}{p}\right)$, but if $y=x$ or $y=p-x$, then it will give $(p-1)\left(\frac{xy}{p}\right)$, therefore it follows that

$$d(S(1))^2+d(S(L))^2=4pd, \qquad \text{i. e.} \quad p=\left(\frac{1}{2}S(1)\right)^2+\left(\frac{1}{2}S(L)\right)^2.$$

The lemma is proved. □

Let us return to the proof of the theorem. In representation (1.4) of p as sum of two integral squares, with $\left(\frac{L}{p}\right)=-1$, we have $S(L)\equiv 0 \pmod 4$, because the summands of $S(L)$ corresponding to different modulo p residues x, $-x$, L/x, $-L/x$ are equal to each other. It follows that the second term in the representation (1.4) is even, while the first term therefore is odd and we can write

$$\left(\frac{1}{2}S(L)\right)^2=A^2, \qquad \left(\frac{1}{2}S(1)\right)^2=B^2. \tag{1.5}$$

According to (1.3), the binomial theorem, and Fermat small theorem we have the following congruences modulo p

$$S(1)\equiv\sum_{x=0}^{p-1}(x(x^2+1))^{\frac{p-1}{2}}=\sum_{x=0}^{p-1}\sum_{\substack{a+b=\frac{p-1}{2},\\ a,b\geqslant 0}}\binom{\frac{p-1}{2}}{a}x^{3a+b}$$

$$= \sum_{\substack{a+b=\frac{p-1}{2},\\ a,b\geqslant 0}} \binom{\frac{p-1}{2}}{a} \sum_{x=0}^{p-1} x^{3a+b} \equiv \sum_{\substack{a+b=\frac{p-1}{2},\\ a,b\geqslant 0}} \binom{\frac{p-1}{2}}{a} \times \begin{cases} 0 & \text{if } 3a+b\neq p-1, \\ -1 & \text{if } 3a+b=p-1 \end{cases}$$

$$= -\binom{\frac{p-1}{2}}{\frac{p-1}{4}} = -\frac{\left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{4}\right)!\left(\frac{p-1}{4}\right)!} \pmod p, \tag{1.6}$$

since the conditions $3a + b = 2a + 2b = p - 1$ imply that $a = b = \frac{p-1}{4}$. From the Wilson theorem we get the congruence

$$-1 \equiv 1 \times \cdots \times \frac{p-1}{2}\left(p - \frac{p-1}{2}\right) \times \cdots \times (p-1)$$

$$\equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p. \tag{1.7}$$

From this congruence and congruence (1.6) we get the congruences

$$B^2 = \left(\frac{1}{2}S(1)\right)^2 \equiv \frac{1}{4}\frac{\left(\left(\frac{p-1}{2}\right)!\right)^2}{\left(\left(\frac{p-1}{4}\right)!\right)^4} \equiv \frac{-1}{4\left(\left(\frac{p-1}{4}\right)!\right)^4} \pmod p,$$

which is the second congruence of (1.1). The first congruence (1.1) follows, since $A^2 = p - B^2$. □

§2. Sums of square and tripled square

Here we shall consider representations of prime numbers p, $p \equiv 1 \pmod 6$, in the form

$$p = T_0^2 + 3T_1^2 \tag{2.1}$$

with integral T_0 and T_1.

Lemma 2. *Let p be a prime number, $p \equiv 1 \pmod 6$ and η a cubic non residue* $\bmod p$. *Then the sums of Legendre symbols*

$$S_l = \sum_{x=0}^{p-1} \left(\frac{x^3 + \eta^{2l}}{p}\right)$$

for $l = 0, 1, 2$ satisfy the relation

$$p = \frac{1}{4}\left(S_0^2 + 3\left(\frac{S_1 - S_2}{3}\right)^2\right). \tag{2.2}$$

Besides, the sum S_0 is even and $S_1 \equiv S_2 \pmod 6$.

Proof. Compare to [1], Lemma 1. Note that if β runs all quadratic residues modulo p, then the set of residues $\beta^3, \eta^2\beta^3, \eta^4\beta^3$, also contains all quadratic residues modulo p, and each quadratic residue is contained in this set exactly three times. Therefore we obtain

$$\frac{p-1}{2}(S_0+S_1+S_2)$$

$$= \sum_{\beta, \left(\frac{\beta}{p}\right)=1} \left(\sum_x \left(\frac{x^3+\beta^3}{p}\right) + \sum_x \left(\frac{x^3+\eta^2\beta^3}{p}\right) + \sum_x \left(\frac{x^3+\eta^4\beta^3}{p}\right) \right)$$

$$= 3 \sum_{z, \left(\frac{z}{p}\right)=1} \sum_{x=0}^{p-1} \left(\frac{x^3+z}{p}\right) = \frac{3}{2} \sum_{x,z=0}^{p-1} \left(\frac{x^3+z^2}{p}\right),$$

from which, by easy formulas

$$\sum_{z=0}^{p-1} \left(\frac{z^2+\beta}{p}\right) = \begin{cases} p-1 & \textit{if} \quad \beta \equiv 0 \pmod p \\ -1 & \textit{otherwise}, \end{cases} \tag{2.3}$$

we obtain the relation

$$S_0+S_1+S_2 = \frac{2}{(p-1)} \frac{3}{2}((p-1)-(p-1)) = 0. \tag{2.4}$$

Similarly, we have

$$\frac{p-1}{3}(S_0^2+S_1^2+S_2^2) = \sum_{\beta=1}^{p-1} \left(\sum_{x=0}^{p-1} \left(\frac{x^3+\beta}{p}\right) \right)^2$$

$$= \sum_{x,y=0}^{p-1} \sum_{\beta=1}^{p-1} \left(\frac{(\beta+x^3)(\beta+x^3+(y^3-x^3))}{p}\right)$$

$$= \sum_{x,y=0}^{p-1} \sum_{z=0}^{p-1} \left(\frac{z(z+(y^3-x^3))}{p}\right),$$

whence, by formulas (2.3), we get

$$\frac{p-1}{3}(S_0^2+S_1^2+S_2^2) = 2(p-1)p,$$

so that

$$S_0^2+S_1^2+S_2^2 = 6p. \tag{2.5}$$

Then from (2.4) and (2.5) we get

$$S_0S_1 + S_0S_2 + S_1S_2 = \frac{1}{2}\left((S_0 + S_1 + S_2)^2 - (S_0^2 + S_1^2 + S_2^2)\right) = -3p,$$

which gives

$$S_0^2 - S_1S_2 = 3p + S_0(S_0 + S_1 + S_2) = 3p.$$

Finally we get

$$S_0^2 + 3\left(\frac{S_1 - S_2}{3}\right)^2 = \frac{1}{3}\big(S_0^2 + S_1^2 + S_2^2 + 2(S_0^2 - S_1S_2)\big) = 4p.$$

If x and $1/x$ are different modulo p, then the corresponding terms of S_0 are either equal or differ by sign, and in any case their sum is even. Otherwise, $x = 0$, or $x = \pm 1$, and the sum of the corresponding terms of S_0 is

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{0}{p}\right) = 1 + \left(\frac{2}{p}\right),$$

i.e. it is even. □

Theorem 2. *Let p be a prime number, $p \equiv 1 \pmod 6$. Then p can be presented in the form* (2.1) *with integral T_0 and T_1 satisfying the congruences*

$$T_0^2 \equiv \frac{(-1)^{\frac{p+1}{2}}}{4\big((\frac{p-1}{3})!\big)^2\big((\frac{p-1}{6})!\big)^2} \pmod p, \quad T_1^2 \equiv \frac{(-1)^{\frac{p-1}{2}}}{12\big((\frac{p-1}{3})!\big)^2\big((\frac{p-1}{6})!\big)^2} \pmod p.$$

Corollary 1. *A prime number p, $p \equiv 1 \pmod 6$, has the form $1 + 3T^2$ with integral T if and only if it satisfies the congruence*

$$4\left(\left(\frac{p-1}{3}\right)!\right)^2\left(\left(\frac{p-1}{6}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Corollary 2. *A prime number p, $p \equiv 1 \pmod 6$, has the form $T^2 + 3$ with integral T if and only if it satisfies the congruence*

$$12\left(\left(\frac{p-1}{3}\right)!\right)^2\left(\left(\frac{p-1}{6}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

Proof. It follows from Lemma 2 that each prime number p satisfying $p \equiv 1 \pmod 6$ can be written in the form (2.1) with integral $T_0 = S_0/2$ and $T_1 = (S_1 - S_2)/6$.

According to definition, the binomial theorem, and Fermat small theorem, we obtain the congruences

$$S_0 \equiv \sum_{x=0}^{p-1} \left(x^3+1\right)^{\frac{p-1}{2}} \equiv \sum_{x=0}^{p-1} \sum_{a=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{a} x^{3a}$$

$$\equiv \sum_{a=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{a} \sum_{x=0}^{p-1} x^{3a} \equiv \sum_{a=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{a} \times \begin{cases} 0 & \text{if} \quad a \neq (p-1)/3, \\ -1 & \text{if} \quad a = (p-1)/3 \end{cases}$$

$$\equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{3}} = -\frac{(\frac{p-1}{2})!}{(\frac{p-1}{3})!(\frac{p-1}{6})!} \pmod{p}.$$

It follows from this congruence and congruence (1.7) that

$$T_0^2 = \left(\frac{1}{2}S_0\right)^2 \equiv \frac{(-1)^{\frac{p+1}{2}}}{4\left((\frac{p-1}{3})!\right)^2 \left((\frac{p-1}{6})!\right)^2} \pmod{p}.$$

Finally, since $3T_1^2 \equiv -T_0^2 \pmod{p}$, we obtain

$$T_1^2 \equiv \frac{(-1)^{\frac{p-1}{2}}}{12\left((\frac{p-1}{3})!\right)^2 \left((\frac{p-1}{6})!\right)^2} \pmod{p}.$$

The corollaries obviously follow from the theorem. □

References

1. A. N. Andrianov, *Representations of integers by some quadratic forms in connection with the theory of elliptic curves.*— Izv. Akad. Nauk SSSR, Ser. mat. **29** (1965), No. 1, 227–238.
2. I. M. Vinogradov, *Basic Number Theory.* M., Nauka, 1981.

St.Petersburg Department
of the Steklov Mathematical
Institute, Russian Academy
of Sciences, Fontanka 27,
191023, St.Petersburg, Russia
E-mail: anandr@pdmi.ras.ru,
anatoli.andrianov@gmail.com

Поступило 25 ноября 2014 г.