FERMAT'S TWO SQUARES THEOREM AND QUARTIC RESIDUACITY

ROLAND BACHER AND GERGELY HARCOS

This note grew out from a discussion at MathOverflow [1].

Theorem 1. *Let $p = x^2 + y^2$ be a prime number with x odd and y divisible by four.*

(a) If $p \equiv 1 \pmod{16}$, then x and y are quartic residues modulo p.
(b) If $p \equiv 9 \pmod{16}$, then y is a quartic residue modulo p, and x is not.

We shall derive this result from the following more general theorem.

Theorem 2. *Let $p = x^2 + y^2$ be a prime number with x odd and y divisible by four.*

(a) The odd divisors of y are quartic residues modulo p.
(b) A divisor of x is a quartic residue modulo p if and only if it is $\equiv \pm 1 \pmod 8$.

This theorem follows readily from Emma Lehmer's criterion for quartic residuacity [3, Page 24], but we prefer to give an idependent proof based on quartic reciprocity in Gaussian integers. In particular, we shall rely on Theorem 2, Proposition 9.8.5, and Proposition 9.8.6 from [2, Chapter 9].

Proof of Theorem 2. Without loss of generality, $x \equiv 1 \pmod 4$. Observe that -1 is a fourth power in $\mathbb{F}_p^\times$, because $p \equiv 1 \pmod 8$.

Let d be an odd divisor of y. Let $d^* = \pm d$ such that $d^* \equiv 1 \pmod 4$. Then d^* and $x+yi$ are primary elements of $\mathbb{Z}[i]$, hence

$$\left(\frac{d^*}{x+yi}\right)_4 = \left(\frac{x+yi}{d^*}\right)_4 = \left(\frac{x}{d^*}\right)_4 = 1.$$

Therefore d^* is a fourth power in $\mathbb{F}_p^\times$, and the same is true of d.

Let d be a divisor of x. Let $d^* = \pm d$ such that $d^* \equiv 1 \pmod 4$. Then d^* and $x+yi$ are primary elements of $\mathbb{Z}[i]$, hence

$$\left(\frac{d^*}{x+yi}\right)_4 = \left(\frac{x+yi}{d^*}\right)_4 = \left(\frac{yi}{d^*}\right)_4 = \left(\frac{i}{d^*}\right)_4 = (-1)^{(d^*-1)/4}.$$

Therefore d^* is a fourth power in $\mathbb{F}_p^\times$ if and only if $d^* \equiv 1 \pmod 8$, and d is a fourth power in $\mathbb{F}_p^\times$ if and only if $d \equiv \pm 1 \pmod 8$. □

Proof of Theorem 1. Observe that y/x has order four in the cyclic group $\mathbb{F}_p^\times$. Observe also that x is a square in $\mathbb{F}_p^\times$ by quadratic reciprocity:

$$\left(\frac{x}{p}\right) = \left(\frac{p}{x}\right) = \left(\frac{x^2+y^2}{x}\right) = \left(\frac{y^2}{x}\right) = 1.$$

Hence the elements of $\{y/x, x, y\} \subset \mathbb{F}_p^\times$ are squares, and we shall examine when they are fourth powers.

Assume that $p \equiv 1 \pmod{16}$. Then y/x is a quartic residue. Moreover, $x \equiv \pm 1 \pmod 8$, hence x is a quartic residue by Theorem 2. It follows that y is a quartic residue.

Assume that $p \equiv 9 \pmod{16}$. Then y/x is not a quartic residue. Moreover, $x \equiv \pm 3 \pmod 8$, hence x is not a quartic residue by Theorem 2. It follows again that y is a quartic residue. □

REFERENCES

[1] R. Bacher, G. Harcos, Discussion at MathOverflow, https://mathoverflow.net/questions/466706

[2] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics, Vol. 84. Springer-Verlag, New York, 1990.

[3] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

UNIV. GRENOBLE ALPES, INSTITUT FOURIER, F-38000 GRENOBLE, FRANCE
Email address: roland.bacher@univ-grenoble-alpes.fr

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, POB 127, BUDAPEST H-1364, HUNGARY
Email address: gharcos@renyi.hu