ON SUMS OF THREE SQUARES

Neville Robbins

Mathematics Department, San Francisco State University, San Francisco, CA 94132

e-mail: robbins@math.sfsu.edu

(Submitted September 2003-Final Revision January 2004)

ABSTRACT

It is known that (1) if the prime $p \equiv 3 \pmod 4$, then a multiple of p is a sum of three squares. (This fact is needed in a proof of Lagrange's four square theorem.) In this note, we present a constructive proof of (1).

Let S_4 denote the set of all natural numbers that can be represented as a sum of four squares of non-negative integers. A well-known theorem of Lagrange states that $S_4 = N$, that is, every natural number can be so represented. (See [1], p. 302.) It is easily seen that $1 \in S_4$, $2 \in S_4$. Furthermore, if $m \in S_4$ and $n \in S_4$, then $mn \in S_4$. Therefore, in order to prove Lagrange's four-square theorem, it suffices to show that every odd prime is a sum of four squares. If the prime $p \equiv 1 \pmod 4$, then p is a sum of two squares (and thus also a sum of four squares). Therefore, we can confine our attention to primes $p \equiv 3 \pmod 4$. If we can show that a multiple of p is a sum of three squares (and therefore also a sum of four squares), then using well-known techniques, we can find a smaller multiple of p that is a sum of four squares.

In view of the above, a key ingredient in the proof of Lagrange's four square theorem is Theorem 1 below:

Theorem 1: If the prime $p \equiv 3 \pmod 4$, then there exist integers a, b, k such that $a^2 + b^2 + 1 = kp$, with $0 < k < p$.

Remarks: A more general version of Theorem 1 appears as Theorem 87 on p. 70 of [1]. Since the constants a, b satisfy: $0 \le a \le \frac{p-1}{2}$, $0 \le b \le \frac{p-1}{2}$, one can demonstrate a stronger result, namely $0 < k \le \frac{p-1}{2}$. Specifically,

$$kp = a^2 + b^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 = \frac{(p-1)^2}{2} + 1 < \frac{p^2}{2} + 1 \ .$$

Therefore

$$kp < \frac{p^2}{2} + 1 \to k < \frac{p}{2} + \frac{1}{p} \to k \le \left[\frac{p}{2} + \frac{1}{p}\right].$$

Since $p \ge 3$, it follows that $\frac{1}{p} < \frac{1}{2}$, so that $\left[\frac{p}{2} + \frac{1}{p}\right] = [\frac{p}{2}] = \frac{p-1}{2}$. The conclusion now follows. $\square$

If the prime p is large, then the process of actually finding the integers a, b becomes cumbersome. We therefore propose Theorem 2 below as an alternative to Theorem 1, with a constructive proof.

Theorem 2: If the prime $p \equiv 3 \pmod 4$, then there exist integers x_1, x_2, x_3, k such that $x_1^2 + x_2^2 + x_3^2 = kp$, with $0 < k < \frac{3p}{4}$.

Proof: Let q be a prime such that $q \not\equiv 3 \pmod 4$ and Legendre symbol $(\frac{q}{p}) = -1$. These conditions are satisfied by all primes, q, such that $q \equiv 2p - 1 \pmod{4p}$. Therefore Dirichlet's theorem on primes in arithmetic progression assures the existence of infinitely many such primes. Since $(\frac{q}{p}) = -1$, Euler's Criterion implies $q^{\frac{p-1}{2}} \equiv -1 \pmod p$, hence $q^{\frac{p+1}{2}} + q \equiv 0 \pmod p$. Since $q \equiv 1 \pmod 4$, it follows that $q = a^2 + b^2$ for integers a, b. Therefore we have

$$(q^{\frac{p+1}{4}})^2 + a^2 + b^2 \equiv 0 \pmod p\,.$$

Next, we find integers x_1, x_2, x_3 such that $x_1 \equiv \pm q^{\frac{p+1}{4}} \pmod p$, $x_2 \equiv \pm a \pmod p$, $x_3 \equiv \pm b \pmod p$ and $|x_i| < \frac{p}{2}$ for all i. This yields $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod p$, hence $x_1^2 + x_2^2 + x_3^2 = kp$, with $kp < \frac{3p^2}{4}$, hence $k < \frac{3p}{4}$. If $k = 0$, then $x_i = 0$ for all i, hence $q \equiv 0 \pmod p$, an impossibility. Therefore $0 < k < \frac{3p}{4}$. □

For example, if $p = 19$, we can take $q = 2 = 1^2 + 1^2$. Then $q^{\frac{p+1}{4}} \equiv 2^5 \equiv 32 \equiv -6 \pmod{19}$. This yields $6^2 + 1^2 + 1^2 = 38 = 2 * 19$.

In general if $p \equiv 3 \pmod 8$, we can take $q = 2$; if $p \equiv 7, 23 \pmod{40}$, we can take $q = 5$. For each of the 13 primes, p, such that $p \equiv 3 \pmod 4$ and $p < 100$, the table below lists the minimum value of q, as well as the corresponding values of x_1, x_2, x_3, k.

p	q	x_1	x_2	x_3	k
3	2	2	1	1	2
7	5	3	2	1	2
11	2	3	1	1	1
19	2	6	1	1	2
23	5	8	2	1	3
31	13	7	3	2	2
43	2	16	1	1	6
47	5	18	2	1	7
59	2	23	1	1	9
67	2	20	1	1	6
71	13	22	3	2	7
79	17	33	4	1	14
83	2	9	1	1	1

REFERENCES

[1] G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*, (4^{th} ed.) Oxford (1960).

AMS Classification Numbers: 11E25

✠ ✠ ✠