

SOME APPLICATIONS OF THUE'S LEMMA

PETE L. CLARK

Recently I learned (from Mariah Hamel) about **Thue's Lemma**, an elementary result about congruences modulo p due to the Norwegian mathematician Axel Thue (1863-1922). I was able to track the result down in several texts – [3, Thm. 11-7], [1, Prop., Ch. 4], [4, Thm. 2.33] – but I believe it is not “well-known”. These texts use Thue's Lemma (only) to prove Fermat's Two Squares Theorem, or more precisely to deduce it from the fact that if $p \equiv 1 \pmod{4}$, then -1 is a square mod p (“Fermat's Lemma”). But there are, of course, many other nice proofs of Fermat's Two Squares Theorem, so if this were the only use of Thue's Lemma then perhaps its relative obscurity would be well-deserved.

The purpose of this short note is to show that in fact Thue's Lemma can be used to prove many other results. Here we concentrate on primes of the form $x^2 + Dy^2$ for a fixed positive integer D , although there are several variants the reader may like to pursue (e.g. $D < 0$ and/or composite values). All of the results we discuss here are classical in a very strong sense: they were first established by Fermat, Euler and/or Lagrange. However, the more traditional proofs require some rudiments of the theory of binary quadratic forms or the arithmetic of quadratic rings, including some technicalities when $\mathbb{Z}[\sqrt{-D}]$ is not the full ring of integers of $\mathbb{Q}(\sqrt{-D})$. The proofs that I present here use only quadratic reciprocity, and seem distinctly more graceful than the traditional ones. Thus I submit to you that Thue's Lemma should appear more prominently in elementary texts and courses.

Lemma 1. (*Thue's Lemma* [5]) *Let p be a prime number and a an integer, with $\gcd(a, p) = 1$. Then there exist integers x and y such that*

- (i) $0 < |x|, |y| < \sqrt{p}$ and
- (ii) $ay \equiv x \pmod{p}$.

Proof. Consider the set $\{au - v \mid u, v \in \mathbb{Z}, 0 \leq u, v \leq \lfloor \sqrt{p} \rfloor\}$. Since there are $\lfloor \sqrt{p} \rfloor^2 > p$ pairs (u, v) , there exists $(u_1, v_1) \neq (u_2, v_2)$ such that

$$au_1 - v_1 \equiv au_2 - v_2 \pmod{p}.$$

Put $x = v_1 - v_2$ and $y = u_1 - u_2$; then (ii) holds. Moreover, $|x|, |y| < \sqrt{p}$, so x (resp. y) is 0 iff it is zero modulo p . By construction x and y are not both 0, and by (ii) if one of them is zero modulo p so is the other. So they are both nonzero. \square

Fix $D \in \mathbb{Z}^+$. The determination of the primes p which are of the form $x^2 + Dy^2$ is a rich classical problem. Just by reducing modulo p , one gets a necessary condition:

Proposition 2. *Let $D \in \mathbb{Z}^+$, and let p be a prime number with $\gcd(D, p) = 1$. If there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + Dy^2$, then $-D$ is a square modulo p .*

It is natural to ask to what extent the converse is true.

Date: August 29, 2009.

Theorem 3. Let $D \in \mathbb{Z}^+$, and let p be an odd prime number such that $\left(\frac{-D}{p}\right) = 1$. Then there exists $k, x, y \in \mathbb{Z}$ with $0 < k \leq D$ and $0 < |x|, |y| < \sqrt{p}$ such that

$$x^2 + Dy^2 = kp.$$

Proof. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv -D \pmod{p}$. Let x, y be integers satisfying the conclusion of Thue's Lemma applied to p and a . Then on the one hand

$$0 < x^2 + Dy^2 < (1 + D)p,$$

while on the other hand

$$x^2 + Dy^2 \equiv (a^2 + D)y^2 \equiv 0 \pmod{p}.$$

□

Taking $D = 1$, we get:

Corollary 4. If p is an odd prime with $\left(\frac{-1}{p}\right) = 1$, then $\exists x, y \in \mathbb{Z}$ with $x^2 + y^2 = p$.

This is essentially Fermat's Two Squares Theorem. To better recognize it, recall Fermat's Lemma: for an odd prime p , -1 is a square modulo p iff $p \equiv 1 \pmod{4}$. We may view Fermat's Lemma as the first case of quadratic reciprocity:

Theorem 5. (Quadratic Reciprocity) Let ℓ and p be distinct odd primes. Put $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$. Then:

- a) $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$.
- b) $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$.
- c) $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

Using Theorem 3 and the other parts of Theorem 5, we can derive further results.

Corollary 6. For an odd prime p , the following are equivalent:

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 2y^2 = p$.
- (ii) $\left(\frac{-2}{p}\right) = 1$.
- (iii) $p \equiv 1, 3 \pmod{8}$.

Proof. We get (ii) \equiv (iii) by using $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ and applying quadratic reciprocity. That (i) \implies (ii) is Proposition 2. To show (ii) \implies (i) we apply Theorem 3, which says that for any prime p satisfying (ii), there exist $x, y \in \mathbb{Z}$ such that either $x^2 + 2y^2 = p$ – done! – or $x^2 + 2y^2 = 2p$. But in the latter case x is even, so we may write $x = 2X$ for an integer X , and then we have $2p = x^2 + 2y^2 = 4X^2 + 2y^2$, so $p = y^2 + 2X^2$. □

Corollary 7. For a prime $p > 3$, the following are equivalent:

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 3y^2 = p$.
- (ii) $\left(\frac{-3}{p}\right) = 1$.
- (iii) $p \equiv 1 \pmod{3}$.

Proof. The equivalence of (ii) and (iii) follows from quadratic reciprocity. Suppose p satisfies (ii) and apply Theorem 3: there exist $x, y \in \mathbb{Z}$ such that $x^2 + 3y^2$ is equal to p , $2p$ or $3p$. In the first case we are done, and the last is handled very much as above: we find that $3 \mid x$, etc. Now consider $x^2 + 3y^2 = 2p$. Reducing mod 3 and using (ii) \equiv (iii), we get $x^2 \equiv 2 \pmod{3}$, a contradiction. □

Corollary 8. *For an odd prime p , the following are equivalent:*

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 4y^2 = p$.
- (ii) $\left(\frac{-4}{p}\right) = 1$.
- (iii) $p \equiv 1 \pmod{4}$.

Proof. Rewriting $x^2 + 4y^2$ as $x^2 + (2y)^2$, the result is seen to be equivalent to the assertion that in Corollary 4, we can take one of x or y to be even. This is certainly true, because if they were both odd, then $x^2 + y^2 = p$ would be even. \square

Corollary 9. *For an odd prime $p \neq 7$, the following are equivalent:*

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 7y^2 = p$.
- (ii) $\left(\frac{-7}{p}\right) = 1$.
- (iii) $p \equiv 1, 2, 4 \pmod{7}$.

Proof. Again (ii) \equiv (iii) follows from quadratic reciprocity: the nonzero squares modulo 7 are 1, 2 and 4. Applying Theorem 3 we get $x^2 + 7y^2 = kp$, for some $1 \leq k \leq 7$. The case $k = 1$ is the favorable one, and $k = 7$ is handled by observing that $7 \mid x$, as above. So we may assume $1 < k < 7$.

Step 1: Reducing modulo 7, we get $x^2 \equiv kp \pmod{7}$. Since $\gcd(7, kp) = 1$ and p is a square modulo 7, it follows that also k is a square modulo 7, i.e., $k = 2$ or $k = 4$.

Step 2: Suppose $x^2 + 7y^2 = 2p$. The possible values of the left hand side mod 8 are 0, 1, 3, 4, 5, 7; the possible values of the right hand side mod 8 are 2, 6: contradiction.

Step 3: Suppose $x^2 + 7y^2 = 4p$. Since the right hand side is even, x and y must have the same parity. If they are both odd, $x^2 + 7y^2 \equiv 0 \pmod{8}$, contradiction. So x and y are both even: $x = 2X$, $y = 2Y$, $4X^2 + 4 \cdot 7Y^2 = 4p$, and $X^2 + 7Y^2 = p$. \square

Why did we skip $D = 5$ and $D = 6$? Because for these values the converse of Proposition 2 is false!

Example 1: Take $D = 5$ and $p = 3$. Then $\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$, but the Diophantine equation $3 = x^2 + 5y^2$ has no solutions.

Example 2: Take $D = 6$ and $p = 5$. Then $\left(\frac{-6}{5}\right) = \left(\frac{4}{5}\right) = 1$, but the Diophantine equation $5 = x^2 + 6y^2$ has no solutions.

In fact one has the following result, first proved by Landau.

Theorem 10. *Let $D \in \mathbb{Z}^+$. Let $\mathcal{P}(D)$ be the set of primes p for which $\left(\frac{-D}{p}\right) = 1$ and the equation $x^2 + Dy^2 = p$ has no \mathbb{Z} -solutions. The following are equivalent:*

- (i) $\mathcal{P}(D)$ is finite.
- (ii) $D = 1, 2, 3, 4, 7$.

Nevertheless, there are further values of D for which Theorem 3 can be used to determine all primes of the form $x^2 + Dy^2$.

Corollary 11. *For an odd prime $p \neq 5$, the following are equivalent:*

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 5y^2 = p$.
- (ii) $\left(\frac{-5}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$.
- (iii) $p \equiv 1, 9 \pmod{20}$.

Proof. Conditions (ii) and (iii) are equivalent by quadratic reciprocity. By Proposition 2, the condition $\left(\frac{-5}{p}\right) = 1$ is necessary for $x^2 + 5y^2 = p$ to have \mathbb{Z} -solutions.

Moreover, the possible values of $x^2 + 5y^2 \equiv x^2 + y^2$ modulo 4 are 0, 1, 2. Since p is odd, we need $p \equiv 1 \pmod{4}$, i.e., $\left(\frac{-1}{p}\right) = 1$. Thus (i) \implies (ii).

Conversely, assume (ii). By Theorem 3, there exists k with $1 \leq k \leq 5$ and $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = kp$. As usual, if $k = 1$ or $k = 5$ we get the desired conclusion. It remains to rule out $k = 2$ and $k = 3$. To see this, reduce modulo 5 to get that kp is a square modulo 5. But $\left(\frac{p}{5}\right)^{\text{QR}} \equiv \left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1 \cdot 1 = 1$, so p is a square mod 5 hence k is a square modulo 5 as well: $k = 1$ or $k = 4$. \square

Corollary 12. *For a prime $p > 5$, the following are equivalent:*

- (i) $\exists x, y \in \mathbb{Z}$ with $x^2 + 6y^2 = p$.
- (ii) $p \equiv 1, 7 \pmod{24}$.

Proof. Assume (i). Reducing modulo 3, we get $p \equiv x^2 \pmod{3}$, so $p \equiv 1 \pmod{3}$. Moreover, $x^2 + 6y^2$ is odd iff x is odd, in which case $x^2 \equiv 1 \pmod{8}$, so that $x^2 + 6y^2 \equiv 1, 7 \pmod{8}$.

Conversely, assume (ii). By Theorem 3, there exists k with $1 \leq k \leq 6$ and $x, y \in \mathbb{Z}$ such that $x^2 + 6y^2 = kp$. Yet again, the result is clear if $k = 1$ or $k = 6$, so assume $1 < k < 6$. Reducing mod 3 we see that k is a square mod 3, so $k = 1, 3, 4$. If $k = 3$, then $3p \equiv 3, 5 \pmod{8}$, which are not values of $x^2 + 6y^2 \pmod{8}$. If $k = 4$, then $4 \mid x^2 + 6y^2$ which implies in turn that $2 \mid x$, $4 \mid x^2$ and $2 \mid y$, so we may put $x = 2X$, $y = 2Y$ and then we get $X^2 + 6Y^2 = p$. \square

We now have seven corollaries to Theorem 3. How many more results are there like this? It turns out that there are only finitely many values of D for which it is possible to answer the question which primes are of the form $x^2 + Dy^2$ purely in terms of congruence conditions.

Theorem 13. *For a positive integer D , the following are equivalent:*

- (i) *There exist coprime positive integers a and N such that every prime number $p \equiv a \pmod{N}$ is of the form $x^2 + Dy^2$.*
- (ii) *Every prime number $p \equiv 1 \pmod{4D}$ is of the form $x^2 + Dy^2$.*
- (iii) *There is a nonempty subset $S \subset (\mathbb{Z}/4D\mathbb{Z})^\times$ such that for a prime number p with $\gcd(p, D) = 1$, p is of the form $x^2 + Dy^2$ iff $p \equiv s \pmod{4D}$ for some $s \in S$.*
- (iv) *$D = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848$, plus possibly one further value of D . If this other value exists, it is at least 10^8 .*

Remark: The 65 values listed in Theorem 13(iv) were discovered by Euler, who called them **numeri idonei**. In English they are called “convenient” or “idoneal” numbers, and they have many other characterizations. Of all things, Euler used them to find large primes, like 1,000,003.

Thus the number of further corollaries (of the type considered above, of course) to Theorem 3 is at most 59. These results are traditionally proved using the elementary theory of binary quadratic forms, c.f. [2]. We leave it to the interested reader to find further cases in which the present methods apply.

REFERENCES

- [1] M. Aigner and G.M. Ziegler, *Proofs from The Book*. Including illustrations by Karl H. Hofmann. Third edition. Springer-Verlag, Berlin, 2004.
- [2] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.
- [3] O. Ore, *Number theory and its history*. Reprint of the 1948 original. With a supplement. Dover Publications, Inc., New York, 1988.
- [4] V. Shoup, *A computational introduction to number theory and algebra*. Second edition. Cambridge University Press, Cambridge, 2009.
- [5] A. Thue, *Et par antydninger ti1 en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. 7 (1902), 57-75.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602, USA
E-mail address: pete@math.uga.edu