

THUE'S LEMMA AND BINARY FORMS

PETE L. CLARK

INTRODUCTION

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 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.

1. THUE'S LEMMA

Theorem 1. (*Thue's Lemma*) *Let $n > 1$ be an integer, and let a be an integer which is relatively prime to n . Then there exist integers x and y such that*

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

Proof. Consider the set $\{au - v \mid u, v \in \mathbb{Z}, 0 \leq u, v \leq \lfloor \sqrt{n} \rfloor\}$. Since there are $(\lfloor \sqrt{n} \rfloor + 1)^2 > n$ pairs (u, v) , there exists $(u_1, v_1) \neq (u_2, v_2)$ such that

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

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

Remark 1: If n is not a perfect square, then of course the inequalities in (i) can be taken to be strict, i.e., $|x|, |y| < \sqrt{n}$.

Date: August 30, 2009.

2. SOME PRELIMINARIES

2.1. Quadratic reciprocity law.

Recall that for an integer n and an odd prime p , the **Legendre symbol** $\left(\frac{n}{p}\right)$ is defined to be 0 if $p \mid n$, 1 if $\gcd(p, n) = 1$ and n is a square modulo p and -1 if n is not a square modulo p .

Theorem 2. (*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) $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

2.2. Representations by $x^2 + Dy^2$.

Fix $D, n \in \mathbb{Z}^+$. We say that n is **of the form** $x^2 + Dy^2$ or is **represented by the form** $x^2 + Dy^2$ if there exist integers x, y such that $x^2 + Dy^2 = n$. If there exist integers (x, y) with $\gcd(x, y) = 1$ such that $x^2 + Dy^2 = n$, then we say n is **primitively represented by $x^2 + Dy^2$** .

Proposition 3. *Let $D, n \in \mathbb{Z}^+$.*

- a) *If n is squarefree, then all representations of n by the form $x^2 + Dy^2$ are primitive.*
- b) *If $\gcd(D, n) = 1$ and n is primitively represented by $x^2 + Dy^2$, then $-D$ is a square modulo n .*

Proof. a) Suppose $n = x^2 + Dy^2$ and $e = \gcd(x, y)$. Then $e^2 \mid n$.

b) Suppose $n = x^2 + Dy^2$, and reduce modulo n : $x^2 \equiv -Dy^2 \pmod{n}$. If y is relatively prime to n , it has an inverse mod n and thus $\frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2 \equiv -D \pmod{n}$. Otherwise, there exists some prime p dividing both y and n , and then $x^2 \equiv -Dy^2 \pmod{n}$ gives $p \mid x$, so the representation is not primitive. \square

For nonsquarefree values of n , we must continue to make a distinction between representations by $x^2 + Dy^2$ and primitive representations by $x^2 + Dy^2$. The following simple result, known already to Euler, is helpful in this regard.

Proposition 4. *Let D, x_1, x_2, y_1, y_2 be positive integers. Then:*

- a) $(x_1x_2 - Dy_1y_2)^2 + D(x_1y_2 + x_2y_1)^2 = (x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2)$.
- b) *If $\gcd(D, (x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2)) = \gcd(x_1, y_1) = \gcd(x_2, y_2) = 1$, then*

$$\gcd(x_1x_2 - Dy_1y_2, x_1y_2 + x_2y_1) = 1.$$

Proof. Direct calculation verifies part a). For part b) \square

Proposition 5. *Let $D \in \mathbb{Z}^+$ and let p be a prime such that $-D$ is not a square modulo p . Suppose $x, y \in \mathbb{Z}$ are such that $p \mid x^2 + Dy^2$. Then $p \mid x$ and $p \mid y$.*

Proof. Let $R = \mathbb{Z}[\sqrt{-D}]$ be the integral domain $\mathbb{Z}[t]/(t^2 + D)$. Any element of R may be expressed as $x + y\sqrt{-D}$ for unique $x, y \in \mathbb{Z}$.

Step 1: We claim that for a prime p such that $-D$ is not a square modulo p , the ideal $(p) = pR$ is a prime ideal of R . Equivalently, the quotient ring R/pR is an integral domain. Now $R/pR = \mathbb{Z}[t]/(t^2 + D, p) = \mathbb{Z}/p\mathbb{Z}[t]/(t^2 + D)$, and that $-D$ is not a square modulo p means precisely that the polynomial $(t^2 + D)$ over the finite field

$\mathbb{Z}/p\mathbb{Z}$ is irreducible. Hence (t^2+D) is a prime ideal of $\mathbb{Z}/p\mathbb{Z}[t]$, so R/pR is a domain.

Step 2: In the ring R we have the factorization

$$x^2 + Dy^2 = (x + \sqrt{-D}y)(x - \sqrt{-D}y).$$

Then $p \mid x^2 + Dy^2$, meaning $(x + \sqrt{-D}y)(x - \sqrt{-D}y) \in pR$. Since pR is prime, one of $x \pm \sqrt{-D}y$ lies in pR . That is, $\frac{x}{p} \pm \sqrt{-D}\left(\frac{y}{p}\right) \in \mathbb{Z}[\sqrt{-D}]$, so $p \mid x$ and $p \mid y$. \square

3. THE MAIN THEOREM AND ITS CONSEQUENCES

Theorem 6. *Let n be a positive integer which is not a perfect square, and let D be a positive integer. Suppose that $\gcd(D, n) = 1$ and that $-D$ is a square modulo n . Then there exist $k, x, y \in \mathbb{Z}$ with $0 < k \leq D$, $0 < |x|, |y| \leq \sqrt{n}$, such that*

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

Proof. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv -D \pmod{n}$. Let x, y be integers satisfying the conclusion of Thue's Lemma applied to n and a . By Remark X.X we have $|x|, |y| < \sqrt{n}$. Then on the one hand

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

while on the other hand

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

\square

Applying Theorem 6 with $D = 1$, we get:

Theorem 7. *Let n be a positive integer such that -1 is a square modulo n . Then there exist integers x and y such that $n = x^2 + y^2$.*

Corollary 8. *A positive integer n is of the form $x^2 + y^2$ iff for every prime $p \equiv 3 \pmod{4}$, $\text{ord}_p(n)$ is even.*

Proof. Certainly $2 = 1^2 + 1^2$ and for any n , $n^2 = n^2 + 0^2$. Also, if $p \equiv 1 \pmod{4}$, then -1 is a square modulo p , so by Theorem 7 p is of the form $x^2 + y^2$. Applying Proposition 4a), it follows that if

(1)

$$n = 2^a p_1^{b_1} \cdots p_r^{b_r} q_1^{2c_1} \cdots q_s^{2c_s}, \quad p_1, \dots, p_r \equiv 1 \pmod{4}, \quad q_1, \dots, q_s \equiv 3 \pmod{4},$$

then n is of the form $x^2 + y^2$. Conversely, suppose $n = x^2 + y^2$, and let p be a prime divisor of n with $p \equiv 3 \pmod{4}$. Then by Proposition 5 we have $p \mid x$, $p \mid y$, so that $p^2 \mid n$ and $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$. Continuing in this way, we arrive at a positive integer k such that $p^{2k} \mid n$ and $\frac{n}{p^{2k}}$ is still of the form $x^2 + y^2$. Doing the same for every $p \equiv 3 \pmod{4}$ which divides n , we see that n is of the form (1). \square

Theorem 9. *Let n be an odd positive integer such that -2 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 2y^2$.*

Proof. We apply Theorem 6 with $N = 2$, getting that there exist integers $x, y \in \mathbb{Z}$ such that either $x^2 + 2y^2 = n$ or $x^2 + 2y^2 = 2n$. In the former case we are done, so assume that $x^2 + 2y^2 = 2n$. Then $2 \mid x$, so we may write $x = 2X$ and obtain $2n = x^2 + 2y^2 = 4X^2 + 2y^2$, so $n = y^2 + 2X^2$. \square

Corollary 10. *A positive integer n is of the form $x^2 + 2y^2$ iff for every prime $p \equiv 5, 7 \pmod{8}$, $\text{ord}_p(n)$ is even.*

The proof of this result – and also the subsequent Corollaries 12, 14 and 16 – is similar to that of Corollary 8. Details are left to the reader.

Theorem 11. *Let n be a positive integer such that $\text{gcd}(12, n) = 1$ and -3 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 3y^2$.*

Proof. Applying Theorem 6, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 3y^2 = kn$ for some k , $1 \leq k \leq 3$. In the first case we are done. In the last case we observe that $3 \mid x$ and proceed as above. It remains to consider the case $x^2 + 3y^2 = 2n$. Reducing modulo 3 we get $x^2 \equiv 2n \pmod{3}$. Let p be any (odd, by hypothesis) prime divisor of n . Then, since -3 is a square mod n , *a fortiori* we have $\left(\frac{-3}{p}\right) = 1$. By quadratic reciprocity, this implies $p \equiv 1 \pmod{3}$. That is, to say, n divisible only by primes of the form $1 \pmod{3}$, from which it follows that $n \equiv 1 \pmod{3}$, and thus $2n \equiv 2 \pmod{3}$. But then $x^2 \equiv 2 \pmod{3}$, a contradiction. \square

Corollary 12. *An odd positive integer n is of the form $x^2 + 3y^2$ iff $\text{ord}_2(n) \neq 1$ and for every prime $p \equiv -1 \pmod{3}$, $\text{ord}_p(n)$ is even.*

Theorem 13. *Let n be an odd positive integer such that -4 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 4y^2$.*

Proof. Taking $x^2 + 4y^2$ as $x^2 + (2y)^2$, we see the result is equivalent to the claim that in the conclusion of Theorem 7, we can take one of x or y to be even. This is certainly true, because if they were both odd, then $x^2 + y^2 = n$ would be even. \square

Corollary 14. *A positive integer n is of the form $x^2 + 4y^2$ iff $\text{ord}_2(n) \neq 1$ and for every prime $p \equiv -1 \pmod{4}$, $\text{ord}_p(n)$ is even.*

Theorem 15. *Let n be a positive integer such that $\text{gcd}(14, n) = 1$ and -7 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 7y^2$.*

Proof. Applying Theorem 6, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 7y^2 = kn$ for some k , $1 \leq k \leq 7$. In case $k = 1$ we are done, and $k = 7$ is handled as usual by observing that $7 \mid x$. So we may assume $1 < k < 7$.

Step 1: Reducing modulo 7, we get $x^2 \equiv kn \pmod{7}$, i.e., kn is a nonzero square modulo 7. Let p be any (odd, by hypothesis) prime divisor of n . Then our hypothesis implies $\left(\frac{-7}{p}\right) = 1$, so by quadratic reciprocity p is a square modulo 7. Therefore n is a product of nonzero squares modulo 7 so it itself a nonzero square modulo 7. Therefore k , being the quotient of nonzero squares modulo 7, is itself a nonzero square modulo 7: i.e., $k = 1, 2, 4$.

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

Step 3: Suppose $x^2 + 7y^2 = 4n$. 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

Corollary 16. *A positive integer is of the form $x^2 + 7y^2$ iff $\text{ord}_2(n) \neq 1$ and for every prime $p \equiv 3, 5, 6 \pmod{7}$, $\text{ord}_p(n)$ is even.*

Why did we skip $D = 5$ and $D = 6$? Because for these values the converse of Proposition 3 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. More generally, reducing mod 20 shows:

Proposition 17. *Let p be a prime such that $\gcd(20, p) = 1$. If there exist $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = p$, then $p \equiv 1, 9 \pmod{20}$.*

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. More generally, reducing mod 24 shows:

Proposition 18. *Let p be a prime such that $\gcd(10, p) = 1$. If there exist $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = p$, then $p \equiv 1, 7 \pmod{24}$.*

Remarkably, simply by taking these auxiliary congruence conditions into account, the above methods can be extended to derive results for these values of D .

Theorem 19. *Let n be a positive integer with $\gcd(10, n) = 1$. Suppose that -1 and -5 are both squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 5y^2$.*

Proof. Applying Theorem 6, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = kn$ for some k , $1 \leq k \leq 5$. As above, the case $k = 5$ reduces to $k = 1$.

Step 1: Reducing modulo 5, we get $x^2 \equiv kn \pmod{5}$, i.e., kn is a nonzero square modulo 5. Let p be any (odd, by hypothesis) prime divisor of n . Then our hypothesis implies $\left(\frac{-5}{p}\right) = 1$, so by quadratic reciprocity p is a square modulo 5. Therefore n is a product of nonzero squares modulo 5 so it itself a nonzero square modulo 5. Therefore k , being the quotient of nonzero squares modulo 5, is itself a nonzero square modulo 5: i.e., $k = 1, 4$.

Step 2: Suppose that $x^2 + 5y^2 = 4n$. We claim that x and y are both even, hence substituting $x = 2X$, $y = 2Y$ gives $X^2 + 5Y^2 = n$. Indeed, this follows simply by considering $x^2 + 5y^2$ modulo 4. \square

Very similar arguments can be used to show the following ‘‘complement’’:

Theorem 20. *Let n be a positive integer with $\gcd(10, n) = 1$. Suppose that for every prime p dividing n , $p \equiv 3, 7 \pmod{20}$. Then there exist $x, y \in \mathbb{Z}$ such that $2n = x^2 + 5y^2$.*

Theorem 21. *Let n be a positive integer with $\gcd(6, n) = 1$. Suppose that every prime divisor of n is congruent to 1 or 7 modulo 24. Then there exist integers x and y such that $n = x^2 + 6y^2$.*

Proof. Applying Theorem 6, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 6y^2 = kn$ for some k , $1 \leq k \leq 6$. As above, the case $k = 5$ reduces to $k = 1$.

Step 1: Reducing modulo 3, we get $x^2 \equiv kn \pmod{3}$, so that $kn \equiv 0, 1 \pmod{3}$. Our hypothesis implies $\left(\frac{-3}{p}\right) = 1$ for all prime divisors of n , so by quadratic reciprocity $p \equiv 1 \pmod{3}$. Thus $n \equiv 1 \pmod{3}$. It follows that $k = 1, 3, 4$.

Step 2: Since -1 is a square modulo 4, quadratic reciprocity implies $n \equiv 1 \pmod{4}$. So if $k = 3$, $3k \equiv 3, 5 \pmod{8}$, which are not values of $x^2 + 6y^2 \pmod{8}$.

Step 3: If $k = 4$, then $4 \mid x^2 + 6y^2$. From this we deduce $2 \mid x$, $4 \mid x^2$ and $2 \mid y$, so we may put $x = 2X$, $y = 2Y$ and then we get $X^2 + 6Y^2 = p$. \square

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