LEGENDRE'S THEOREM, LEGRANGE'S DESCENT

SUPPLEMENT FOR MATH 370: NUMBER THEORY

Abstract. Legendre gave simple necessary and sufficient conditions for the solvablility of the diophantine equation $aX^2 + bY^2 + cZ^2 = 0$ where abc is non-zero and square free: the equation has a non-trivial solution if and only if (i) a, b, c do not all have the same sign, (iia) $-bc$ is a square modulo $|a|$, (iib) $-ac$ is a square modulo $|b|$, and (iic) $-ab$ is a square modulo $|c|$.

In this exposition of Legendre's theorem, we give a proof based on Lagrange's descent procedure for equations of the form $Z^2 = aX^2 + bY^2$. This exposition is intended in part to serve as an introduction to the paper *Counterexamples to the Hasse Principle: an elementary introduction* by W. Aitken and F. Lemmermeyer.

1. Introduction

Let $F(X, Y, Z)$ be a quadratic form with integer coefficients. (A *quadratic form* is a homogeneous polynomial of degree 2). We are interested in determining if there are $\mathbb{Z}$-solutions to the equation $F(X, Y, Z) = 0$. Of course, $(0, 0, 0)$ is trivially a solution; we are interested only in non-trivial solutions $(x_0, y_0, z_0) \neq (0, 0, 0)$.

If one non-trivial solution exists then an infinite number exists, and the general solution can be found using a well-known method for parameterizing the conic. In what follows we will confine our attention to determining whether any non-trivial solutions exist, and ignore the problem of finding the general solution. The key result is Legendre's theorem stated and proved below. The proof employs Lagrange's technique of descent, which not only determines existence or non-existence of solutions, but gives a practical method for finding a solution if it exists. (Lagendre's original proof was different[1], but the technique of using Lagrange's descent to prove Legendre's theorem a traditional one. See, for example, Chapter VII, Section 3 of [1], and Chapter II, §XIV and Chapter IV, Appendix I of [3].)

Since we are considering homogeneous equations, $\mathbb{Z}$-solvability and $\mathbb{Q}$-solvability are seen to be equivalent conditions (one can clear denominators). We will sometimes focus on rational solutions, and sometimes focus on integer solutions. If there is a common factors in an integer solution we can remove it. A *primitive triple* (x_0, y_0, z_0) is a triple of integers, not all zero, whose greatest common divisor (GCD) is 1. So if there is a non-trivial $\mathbb{Z}$-solution or $\mathbb{Q}$-solution then there is a primitive $\mathbb{Z}$-solution:

Lemma 1. *The following conditions are equivalent:*
(i) $F(X, Y, Z) = 0$ has a non-trivial $\mathbb{Q}$-solution.
(ii) $F(X, Y, Z) = 0$ has a non-trivial $\mathbb{Z}$-solution.
(iii) $F(X, Y, Z) = 0$ has a primitive $\mathbb{Z}$-solution.

[1]That is, if I understand Weil's remarks after the statement of this theorem in Chapter IV, §VI of [3].

2. Preliminary reduction using linear algebra

Let $k = \mathbb{Q}$, or more generally a field k of characteristic not equal to 2 (i.e., we require that $1 + 1 \neq 0$ in k). Every quadratic form in $k[X_1, \ldots, X_n]$ can be written as $\overrightarrow{X} A \overrightarrow{X}^t$ where A is a symmetric matrix with entries in k and where $\overrightarrow{X} = [X_1, X_2, \ldots, X_n]$ is the row vector with variable entries. Basic linear algebra gives a method for finding a non-singular n by n matrix M with entries in k such that $M^t A M$ is diagonal (see Theorem 1′, Chapter IV, of [2]). In the case where $k = \mathbb{Q}$, we can choose this M so that $M^t A M$ has entries in $\mathbb{Z}$.

Let A be a matrix representing the quadratic form $F(X, Y, Z)$ and let $M^t A M$ be a diagonal matrix with diagonal coefficients $a, b, c \in \mathbb{Z}$. Then the matrix M gives a bijection between (i) the set of non-trivial $\mathbb{Q}$-solutions of $aX^2 + bY^2 + cZ^2 = 0$ and (ii) the set of non-trivial F-solutions of $F(X, Y, Z) = 0$. By Lemma 1, the diophantine equation $F(X, Y, Z) = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution.

If a, b, or c is zero, then we easily find non-trivial $\mathbb{Z}$-solutions. So from now on *assume*

$$F(X, Y, Z) = aX^2 + bY^2 + cZ^2$$

where $a, b, c \in \mathbb{Z}$ are each non-zero.

3. normal forms

There are two normal forms of special interest. The first is the case were $c = -1$ and where a and b are square free. In this case,

$$Z^2 = aX^2 + bY^2$$

is said to be in *Lagrange normal form*.

The second normal form results from the case where the product abc is square-free. In this case, $aX^2 + bY^2 + cZ^2 = 0$ is said to be in *square-free normal form*.[2]

We now show that we can always reduce our equations to these normal forms.

Lemma 2. *Suppose $c \in \mathbb{Z}$ is non-zero. The map $(x_0, y_0, z_0) \mapsto (x_0, y_0, cz_0)$ is a bijection from (i) the set of $\mathbb{Q}$-solutions of $aX^2 + bY^2 + cZ^2 = 0$ to (ii) the set of $\mathbb{Q}$-solutions of $acX^2 + bcY^2 + Z^2 = 0$.*

Using Lemma 1, we get the following corollary of the above lemma:

Corollary 1. *The equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if $acX^2 + bcY^2 + Z^2 = 0$ does.*

Lemma 3. *Suppose $d^2 \mid a$. Then the map $(x_0, y_0, z_0) \mapsto (dx_0, y_0, z_0)$ is a bijection from the set of $\mathbb{Q}$-solutions of $aX^2 + bY^2 + cZ^2 = 0$ to the set of $\mathbb{Q}$-solutions of $(a/d^2)X^2 + bY^2 + cZ^2 = 0$.*

Corollary 2. *Suppose $d^2 \mid a$. Then the equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if $(a/d^2)X^2 + bY^2 + cZ^2 = 0$ does.*

A consequence of the above two corollaries is that we can always transform our equation to Lagrange normal form. To get an equation into square-free normal form, we need the following:

[2] I was tempted to call it *Legendre normal form*, but I found that confusing.

Lemma 4. *Suppose $d \mid a$ and $d \mid b$. Then the map $(x_0, y_0, z_0) \mapsto (dx_0, dy_0, z_0)$ is a bijection from the set of projective solutions of $aX^2 + bY^2 + cZ^2 = 0$ to the set of projective solutions of $(a/d)X^2 + (b/d)Y^2 + cdZ^2 = 0$.*

Corollary 3. *Suppose $d \mid a$ and $d \mid b$. Then the equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if $(a/d)X^2 + (b/d)Y^2 + cdZ^2 = 0$ does.*

To convert $aX^2 + bY^2 + cZ^2 = 0$ to square-free normal form, first divide by the GCD of a, b, c giving a new equation where the GCD of a, b, c is one. Next, using Corollary 2, we can transform the equation to the case where that a, b, c are square-free. Now suppose two of the coefficients, a and b say, are divisible by a prime p. By Corollary 3, we can reduce the problem of solving $aX^2 + bY^2 + cZ^2 = 0$ to that of solving $a'X^2 + b'Y^2 + c'pZ^2 = 0$ where $a' = a/p$, $b' = b/p$ and $c' = pc$. Since a, b were square free, a' and b' are not divisible by p and are also square free. Also c' is square free since p does not divide c. By continuing this process for each p whose square divides abc, we reduce to the case where $aX^2 + bY^2 + cZ^2 = 0$ is in square-free normal form.

4. NECESSARY CONDITIONS

First consider the case where the equation is in Lagrange normal form.

Proposition 1. *If $Z^2 = aX^2 + bY^2$ has a non-trivial $\mathbb{Z}$-solution, then*
(i) at least one of a and b is positive,
(ii) a is a square modulo $|b|$,
(iii) b is a square modulo $|a|$, and
(iv) $-(a/d)(b/d)$ is a square modulo d where d is the GCD of a and b.

Proof. The condition (i) is clear from the fact that all $\mathbb{Z}$-solutions are $\mathbb{R}$-solutions.

By Lemma 1 we can assume that $z_0^2 = ax_0^2 + by_0^2$ where (x_0, y_0, z_0) is primitive. Any common prime divisor p of x_0 and b also divides z_0. But then p^2 divides by_0^2. Since b is square free, p divides y_0, a contradiction. Thus x_0 is prime to b and $a \equiv \left(z_0 x_0^{-1}\right)^2 \bmod b$. This gives (ii). Of course, (iii) follows as well.

Now observe that d^2 divides z_0^2, so d divides z_0. Thus

$$d\left(\frac{z_0}{d}\right)^2 = \left(\frac{a}{d}\right)x_0^2 + \left(\frac{b}{d}\right)y_0^2,$$

so

$$-\left(\frac{a}{d}\right)\left(\frac{b}{d}\right) \equiv \left(\frac{b}{d}y_0 x_0^{-1}\right)^2 \mod d,$$

since, as we saw, x_0 is prime to b and consequently to d. □

Now we consider equations in square-free normal form.

Proposition 2. *Suppose $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution where abc is square-free. then (i) a, b, c are not all of the same sign, (iia) $-bc$ is a square modulo $|a|$, (iib) $-ac$ is a square modulo $|b|$, and (iic) $-ab$ is a square modulo $|c|$.*

Proof. The first condition is clear from the fact that all $\mathbb{Z}$-solutions are $\mathbb{R}$-solutions. For the second condition it suffices to prove (iia).

By Lemma 1 we can assume that $ax_0^2 + by_0^2 + cz_0^2 = 0$ where (x_0, y_0, z_0) is primitive. Observe that $-by_0^2 \equiv cz_0^2 \bmod |a|$. Next observe that a and y_0 are relatively prime: otherwise, if p is a prime dividing both, then p must divide cz_0^2. But a and c are

relatively prime, so p must divide z_0. But then p^2 must divide ax_0^2. Since a is square free, p must divide x_0 contradicting the GCD 1 condition on (x_0, y_0, z_0).

Thus y_0 has an inverse modulo $|a|$ and $-bc \equiv \left(cz_0y_0^{-1}\right)^2 \bmod |a|$. □

5. Lagrange's Descent and the main Theorem

Rational numbers of the form a^2+nb^2 and a^2-nb^2 can be regarded as products of numbers in quadratic extensions of $\mathbb{Q}$. For example,

$$u^2 + 5v^2 = \left(u + \sqrt{-5}v\right)\left(u - \sqrt{-5}v\right).$$

Such factorizations motivate a variety of classical algebraic identities involving sums or differences of squares. An example is the following:

Lemma 5. *Suppose $a, b, b', e \in \mathbb{Z}$ are such that $a + bb'e^2$ is a square and $bb'e^2 \neq 0$. Then $Z^2 = aX^2 + bY^2$ has a non-trivial $\mathbb{Q}$-solution if and only if $Z^2 = aX^2 + b'Y^2$ does.*

Proof. By symmetry, it suffices to prove one direction of the biconditional. Suppose (x_0, y_0, z_0) is a non-trivial $\mathbb{Q}$-solution to $Z^2 = aX^2 + bY^2$. So

$$by_0^2 = z_0^2 - ax_0^2 = \left(z_0 + x_0\sqrt{a}\,\right)\left(z_0 - x_0\sqrt{a}\,\right)$$

(for a fixed choice of square root $\sqrt{a} \in \mathbb{C}$).

Now write $a + bb'e^2 = u^2$. So

$$bb'e^2 = u^2 - a = \left(u + \sqrt{a}\right)\left(u - \sqrt{a}\right).$$

Combining we get

$$\begin{aligned}
b'(bey_0)^2 &= (bb'e^2)(by_0^2) \\
&= \left(u + \sqrt{a}\right)\left(u - \sqrt{a}\right)\left(z_0 + x_0\sqrt{a}\right)\left(z_0 - x_0\sqrt{a}\right) \\
&= \left(u + \sqrt{a}\right)\left(z_0 + x_0\sqrt{a}\right)\left(u - \sqrt{a}\right)\left(z_0 - x_0\sqrt{a}\right) \\
&= \Big((uz_0 + ax_0) + (ux_0 + z_0)\sqrt{a}\Big)\Big((uz_0 + ax_0) - (ux_0 + z_0)\sqrt{a}\Big) \\
&= (uz_0 + ax_0)^2 - a(ux_0 + z_0)^2.
\end{aligned}$$

So $(ux_0 + z_0,\ bey_0,\ uz_0 + ax_0)$ is a $\mathbb{Q}$-solution to $Z^2 = aX^2 + b'Y^2$. Since

$$\begin{bmatrix} u & 0 & 1 \\ 0 & be & 0 \\ a & 0 & u \end{bmatrix}$$

has determinant $be(u^2 - a) = be(bb'e^2) \neq 0$, the above solution to $Z^2 = aX^2 + b'Y^2$ is non-trivial. □

The necessary conditions of Proposition 1 turn out to be sufficient conditions to execute a descent:

Definition 1. We will say that (a, b) satisfies the *descent condition* when (i) a, b are square-free non-zero integers not both negative, (ii) a is a square modulo $|b|$, (iii) b is a square modulo $|a|$, and (iv) $-(a/d)(b/d)$ is a square modulo d where d is the GCD of a and b.

Lemma 6. *Suppose that a, b, b', e are non-zero integers such that $a + bb'e^2$ is a square, but where a, b, b' are square-free. If the pair (a, b) satisfies the descent conditions, then so does (a, b').*

Proof. Write $a + bb'e^2 = u^2$. If a and b' are both negative, then b must be positive since (a, b) satisfies the descent condition. This implies u^2 is negative, a contradiction. Thus (a, b') satisfy the first condition. The second condition, that a is a square modulo $|b'|$, is clear from the equation $a + bb'e^2 = u^2$.

To continue, we need to consider four classes of primes (really three). In what follows, let d be the GCD of a and b and let d' be the GCD of a and b'.

TYPE 1: p a prime dividing a but not $bb'e^2$. Then $b' \equiv b^{-1}\left(e^{-1}u\right)^2 \bmod p$, and so b' is a square modulo p since b is a square modulo p.

TYPE 2: p a prime dividing a and b. In other words, $p \mid d$. Thus $p \mid u$, since $u^2 = a + bb'e^2$. However, $p \nmid b'$ and $p \nmid e$ since a is square free and $a = u^2 - bb'e^2$. By assumption, $-(a/d)(b/d)$ is a square modulo d and a and b are square free, so $-(a/p)(b/p)$ must be a non-zero square modulo p. Divide both sides of the equation $u^2 = a + bb'e^2$ by p, then multiply by a/p:

$$a\left(\frac{u}{p}\right)^2 = \frac{a}{p}\frac{u^2}{p} = \frac{a}{p}\cdot\frac{a + bb'e^2}{p} = \left(\frac{a}{p}\right)^2 - \left(-\frac{a}{p}\frac{b}{p}\right)b'e^2.$$

The left hand side of this equation is divisible by p. Solving for b' modulo p shows that b' is a square modulo p.

TYPE 3: p a prime dividing a and b'. In other words, $p \mid d'$. So b' is trivially a square modulo p. Now $p \mid u$ since $u^2 = a + bb'e^2$. However, $p \nmid b$ and $p \nmid e$ since a is square free and $a = u^2 - bb'e^2$. Now

$$\frac{a}{p} + \left(\frac{b'}{p}\right)be^2 = p\left(\frac{u}{p}\right)^2 \quad \text{so} \quad -\left(\frac{a}{p}\frac{b'}{p}\right)be^2 \equiv \left(\frac{a}{p}\right)^2 \mod p.$$

Since b and e^2 are non-zero square modulo p, it follows that $-(a/p)(b'/p)$ is a square modulo p. From this it follows that $-(a/d')(b/d')$ is a square modulo p.

TYPE 4: p a prime dividing a and e. Now $p \mid u$ since $u^2 = a + bb'e^2$. So $p^2 \mid a$ since $a = u^2 - bb'e^2$. But this contradicts the assumption that a is square free, so no such p exists.

By the Chinese Remainder Theorem, if $p_1, \ldots, p_k$ are distinct primes, and if an integer N is a square modulo p_i for each i, then N is a square modulo the product $p_1 \cdots p_k$. Since a is square free, and since b' is a square for all three types of primes dividing a, it follows that b' is a square modulo $|a|$, and the third requirement holds for (a, b'). By considering only primes of the third type, we get $-(a/d')(b/d')$ is a square modulo d'. So the fourth and final requirement holds for (a, b'). □

Theorem 1. *Suppose that $a, b \in \mathbb{Z}$ are integers such that (a, b) satisfies the descent condition. Then $Z^2 = aX^2 + bY^2$ has a non-trivial $\mathbb{Z}$-solution.*

Proof. Observe that if $a = 1$ then $(1, 1, 0)$ is a non-trivial solution, and if $b = 1$ then $(1, 0, 1)$ is a non-trivial solution. Our goal is to use descent until we get to an equation with $a = 1$ or $b = 1$.

For convenience, suppose that $|a| \leq |b|$. If $|a| = |b| = 1$ we are done since either a or b must be positive. So assume that $|b| \geq 2$.

Since (a, b) satisfies the descent condition, a is a square modulo $|b|$. Let u be an integer of smallest absolute value so that $a \equiv u^2 \bmod |b|$. In other words, $|u| \leq |b|/2$, and b divides $u^2 - a$. Write $u^2 - a = bb'e^2$ where b' is square free.

If $bb'e^2 = 0$, then a is a square. Since a is square free, $a = 1$ and we are done. So from now on assume that b' and e are non-zero.

Claim: $|b'| < |b|$. To see this observe that

$$|b||b'||e^2| = |u^2 - a| \leq |u|^2 + |a| \leq |b|^2/4 + |b|, \qquad \text{so} \qquad |b'| \leq |b|/4 + 1.$$

This gives

$$|b'| \leq |b|/4 + 1 < |b|/4 + 3|b|/4 = |b|.$$

($1 < 3|b|/4$ since we are in the case where $|b| \geq 2$.) By Lemma 5 we have reduced the equation to one with smaller coefficients (their product is smaller in absolute value).

The new equation has coefficients a and b'. These coefficients satisfy the descent condition by the previous lemma. If either is 1 we are done. Otherwise repeat the descent, reducing the problem to an equation with yet smaller coefficients. In this way we continue until one of the coefficients is 1 and we are guaranteed a solution. □

Corollary 4 (Legendre's Theorem)**.** *Suppose $a, b, c \in \mathbb{Z}$ are such that abc is a non-zero square-free integer. Then the equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if (i) a, b, c do not all have the same sign, (iia) $-bc$ is a square modulo $|a|$, (iib) $-ac$ is a square modulo $|b|$, and (iic) $-ab$ is a square modulo $|c|$.*

Proof. One direction has been done (Proposition 2). By Corollary 1, for the other direction it is enough to show that $Z^2 = -acX^2 - bcY^2$ has a non-trivial $\mathbb{Z}$-solution, and by the previous theorem, it is enough to show that $a' = -ac$ and $b' = -bc$ satisfy the descent conditions.

Since abc is a non-zero square-free integer, the same is true of $a' = -ac$ and $b' = -bc$. Since a, b, c are not all of the same sign, either a' or b' is positive. So the first descent condition is satisfied.

By assumption, $a' = -ac$ is a square modulo $|b|$. Trivially, $-ac$ is a square modulo $|c|$. Since b and c are relatively prime (abc is square free), we have that a' is a square modulo $|b'| = |bc|$. So the second descent condition is satisfied. The third is satisfied for similar reasons.

Since abc is square-free, the GCD of $a' = -ac$ and $b' = -bc$ is just $|c|$. And $-(a'/|c|)(b'/|c|) = -ab$ is a square modulo $|c|$ by assumption. So the fourth and final descent condition is satisfied. □

6. Hasse Principle

In this section we consider the congruences

$$aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^k$$

and their relation to the Diophantine equation $aX^2 + bY^2 + cZ^2 = 0$. As before, we assume $a, b, c \in \mathbb{Z}$ are such that abc is non-zero and square-free.

A triple (x_0, y_0, z_0) is said to be *p-primitive* if at least one of x_0, y_0, z_0 is not divisible by p. Now above we saw that primitive $\mathbb{Z}$-solutions had the stronger property that x_0, y_0, z_0 were pairwise relatively prime. With this in mind we say that a solution (x_0, y_0, z_0) to the congruence is *p-strong* if at most one of x_0, y_0, z_0 is divisible by p.

Exercise 1. Show that if $k \geq 2$ then any p-primitive solution to

$$aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^k$$

is automatically a p-strong solution. (Of course this fails if $k = 1$ and $p \mid abc$.)

Exercise 2. Suppose that $p \mid a$ and that the congruence $aX^2+bY^2+cZ^2 \equiv 0 \bmod p$ has a p-strong solution. Show that $-bc$ is a square modulo p.

Conclude that if $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^2$ has a p-primitive solution then $-bc$ is a square modulo p.

Exercise 3. Suppose that, for all $p \mid a$, the congruence $aX^2+bY^2+cZ^2 \equiv 0 \bmod p$ has a p-strong solution. Show that $-bc$ is a square modulo $|a|$.

Conclude that if $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^2$ has a p-primitive solution for all $p \mid a$ then $-bc$ is a square modulo $|a|$.

Exercise 4. Show that in the previous exercise it suffices to have solutions for all *odd* $p \mid a$.

From the above exercises together with Legendre's theorem we get the following

Theorem 2. *Suppose $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p$ has a p-strong solution for all odd $p \mid abc$. Suppose also that $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{R}$-solution. Then $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution.*

Theorem 3. *Suppose $aX^2 + bY^2 + cZ^2 \equiv 0 \bmod p^2$ has a p-primitive solution for all odd $p \mid abc$. Suppose also that $aX^2+bY^2+cZ^2 = 0$ has a non-trivial $\mathbb{R}$-solution. Then $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution.*

Corollary 5 (Hasse Principle: form 1)**.** *The equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if (i) it has a non-trivial $\mathbb{R}$-solution, and (ii) it has a primitive solution modulo p^k for all primes p and integers $k \geq 1$.*

This can be restated using the p-adic integers:

Corollary 6 (Hasse Principle: form 2)**.** *The equation $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial $\mathbb{Z}$-solution if and only if (i) it has a non-trivial $\mathbb{R}$-solution, and (ii) it has a non-trivial $\mathbb{Z}_p$-solution for all primes p.*

The advantage of this statement is that it is obvious that all these conditions are preserved under matrix transformations (as discussed in the second section), so one gets

Corollary 7 (Hasse Principle: form 3)**.** *Consider a quadratic homogeneous Diophantine equation $F(X, Y, Z) = 0$ where $F(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ has degree 2. Then this equation has a non-trivial $\mathbb{Z}$-solution if and only if (i) it has a non-trivial $\mathbb{R}$-solution, and (ii) it has a non-trivial $\mathbb{Z}_p$-solution for all primes p.*

References

[1] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, Dover 1983 (original edition, Hutchinson & Company Ltd, 1952).

[2] J.-P. Serre, *A course in arithmetic*, Springer-Verlag 1973

[3] A. Weil, *Number theory: an approach through history*, Birkhäuser 1984