THE LOCAL-GLOBAL PRINCIPLE

KEITH CONRAD

1. Introduction

Hensel created p-adic numbers near the start of the 20th century and they had some early positive influences: Hensel used them to solve a conjecture of Dedekind about discriminants in algebraic number theory and they directly inspired Steinitz [10] to develop a general theory of fields in order to account for the p-adic numbers alongside previously known fields of numbers and functions. (See [8] for a discussion of Steinitz's paper in English.) Most mathematicians viewed p-adic numbers with suspicion, perhaps in part because of their unclear foundations and Hensel's mistaken proof by p-adic numbers that e is transcendental.

The first indication that the p-adic numbers *for all p together* have a conceptual role in mathematics came in the 1920s when Hasse discovered that Minkowski's work on quadratic forms over the rational numbers could be streamlined by expressing the results in terms of quadratic forms over the real numbers and all p-adic numbers. Hasse became a strong advocate of this point of view for number theory, which came to be called the local-global principle or Hasse principle. Roughly speaking, it states

a theorem or property holds over $\mathbf{Q}$ if and only if it holds over $\mathbf{R}$ and $\mathbf{Q}_p$ for all p

or, more generally,

study a problem over $\mathbf{Q}$ by studying it in $\mathbf{R}$ and all $\mathbf{Q}_p$.

The local-global principle is not a definite theorem, but more of a philosophy. It plays a role comparable in number theory to the idea in geometry of studying global properties of a curve or surface through the local geometric properties near each point on the curve or surface. We call $\mathbf{Q}$ a *global field* and the fields $\mathbf{R}$ and $\mathbf{Q}_p$ *local fields*.[1]

We will see what the local–global principle is about by taking a classical theorem about sums of two squares in the integers and reformulating it as a theorem in $\mathbf{R}$ and every $\mathbf{Z}_p$. A few examples will show the deficiency of working with $\mathbf{Z}_p$ and what is gained by working with $\mathbf{Q}_p$ instead. Then we will state Hasse's version of Minkowski's theorem on quadratic forms over $\mathbf{Q}_p$ as an example where the local–global principle works. Next we will see counterexamples to the local–global principle. Finally we will discuss a local–global result for powers and for heights.

2. Sums of two squares in $\mathbf{Z}$

Here is a classical theorem in number theory about sums of two squares.

Theorem 2.1 (Euler)**.** *A positive integer m can be written as a sum of two squares if and only if each prime p dividing m with $p \equiv 3 \bmod 4$ has even multiplicity as a factor of m.*

[1]More generally, any finite extension of $\mathbf{Q}$ is considered to be a global field and any finite extension of $\mathbf{Q}_p$ is considered to be a local field. The completion of a global field at any nontrivial absolute value is a local field.

Example 2.2. Let $m = 15 = 3 \cdot 5$. Its only prime factor that is congruent to 3 mod 4 is 3, which divides 15 only once. You can check that 15 is not a sum of two squares. The number $m = 45 = 3^2 \cdot 5$ is divisible by 3 two times and $45 = 9 + 36 = 3^2 + 6^2$.

To reformulate Theorem 2.1 in terms of p-adic numbers, we describe when a (nonzero) p-adic integer is a sum of two squares in $\mathbf{Z}_p$.

Theorem 2.3. *For a prime $p \equiv 1 \bmod 4$, every p-adic integer is a sum of two squares of p-adic integers.*

Proof. If $p \equiv 1 \bmod 4$ then a theorem of Fermat from number theory says $-1 \bmod p$ is a square: $-1 \equiv s_0^2 \bmod p$ for some integer s_0. Then Hensel's lemma lifts that up to saying $s^2 + 1 = 0$ has a solution in $\mathbf{Z}_p$: $f(x) = x^2 + 1$ has $f(s_0) \equiv 0 \bmod p$ and $f'(s_0) = 2s_0 \not\equiv 0 \bmod p$.

For each t in $\mathbf{Z}_p$,

$$(1+t)^2 + (s(t-1))^2 = 1 + 2t + t^2 - (t^2 - 2t + 1) = 4t,$$

so $t = ((1+t)/2)^2 + (s(t-1)/2)^2$ and the numbers $(1+t)/2$ and $s(t-1)/2$ are in $\mathbf{Z}_p$ since $p \neq 2$. □

Theorem 2.4. *For a prime $p \equiv 3 \bmod 4$, a nonzero p-adic integer t is a sum of two squares in $\mathbf{Z}_p$ if and only if $\mathrm{ord}_p(t)$ is even.*

Proof. Write $t = p^e u$, with $e \geq 0$ and $u \in \mathbf{Z}_p^\times$.

Step 1: We can write $u = x^2 + y^2$ for some x and y in $\mathbf{Z}_p$.

This will follow from the pigeonhole principle to solve the equation as a congruence mod p first and then from Hensel's lemma to lift the solution mod p to a solution in $\mathbf{Z}_p$. We start by considering the two sets

$$A = \{y^2 \bmod p : 0 \leq y \leq p-1\}, \quad B = \{u - x^2 \bmod p : 0 \leq x \leq p-1\}.$$

For odd prime p, the number of squares in $\mathbf{Z}/(p)$, including 0, is $(p+1)/2$. Therefore $|A| = (p+1)/2$ and $|B| = (p+1)/2$. Since $|A| + |B| = p + 1 > |\mathbf{Z}/(p)|$, the sets A and B must overlap by the pigeonhole principle: there are x_0 and y_0 from 0 to $p-1$ such that $y_0^2 \equiv u - x_0^2 \bmod p$, so $u \equiv x_0^2 + y_0^2 \bmod p$. At least one of x_0 or y_0 is nonzero modulo p. Since the congruence is symmetric in x_0 and y_0 we can assume without loss of generality that $x_0 \not\equiv 0 \bmod p$. Then define

$$f(X) = X^2 + (y_0^2 - u) \in \mathbf{Z}_p[X].$$

We have $f(x_0) \equiv 0 \bmod p$ and $f'(x_0) = 2x_0 \not\equiv 0 \bmod p$, so by Hensel's lemma there is an $x \in \mathbf{Z}_p$ such that $f(x) = 0$, so $x^2 + y_0^2 = u$.

Step 2: e is even.

Write $e = 2k$. Then $t = p^{2k}u = p^{2k}(x^2 + y^2)$ by Step 1, so $t = (p^k x)^2 + (p^k y)^2$.

Step 3: e is odd.

Assuming $t = x^2 + y^2$ in $\mathbf{Z}_p$ we will get a contradiction. Since $\mathrm{ord}_p(t)$ is odd we can't have x or y equal to 0 (otherwise t would be a square, hence of even p-adic valuation). We also must have $\mathrm{ord}_p(x) = \mathrm{ord}_p(y)$, since if the two valuations were not equal then x^2 and y^2 would have different valuations, making $\mathrm{ord}_p(t) = \max(2\,\mathrm{ord}_p(x), 2\,\mathrm{ord}_p(y))$, which is even.

Write $x = p^n v$ and $y = p^n w$ where $n \geq 0$ and v and w are in $\mathbf{Z}_p^\times$. Then

$$t = x^2 + y^2 = p^{2n}(v^2 + w^2).$$

Since $\mathrm{ord}_p(t)$ is odd, v^2+w^2 can't be in $\mathbf{Z}_p^\times$, so $v^2+w^2 \equiv 0 \bmod p$. Thus $v^2 \equiv -w^2 \bmod p$, so $-1 \equiv (v/w)^2 \bmod p$. Therefore -1 is a square in $\mathbf{Z}/(p)$, and it is a classical fact that $-1 \bmod p$ is not a square if $p \equiv 3 \bmod 4$.[2] □

Theorem 2.5. *A nonzero 2-adic integer $2^e u$ with $u \in \mathbf{Z}_2^\times$ is a sum of two squares in $\mathbf{Z}_2$ if and only if $u \equiv 1 \bmod 4$.*

Proof. Case 1: $u \equiv 1 \bmod 4$.

Lifting to modulus 8, either $u \equiv 1 \bmod 8$ or $u \equiv 5 \bmod 8$. Either way we will show u is a sum of two squares in $\mathbf{Z}_2$.

If $u \equiv 1 \bmod 8$ then $u = s^2 = s^2+0^2$ for some $s \in \mathbf{Z}_2$. If $u \equiv 5 \bmod 8$ then $u/5 \equiv 1 \bmod 8$, so $u/5 = s^2$ for some $s \in \mathbf{Z}_2$ and that makes $u = 5s^2 = s^2 + (2s)^2$.

The number $2 = 1+1$ is a sum of two squares, and u is a sum of two squares. A product of sums of two squares is a sum of two squares, from the classical identity

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2,$$

so $2^e u$ is a sum of two squares in $\mathbf{Z}_2$ for all $e \geq 0$.

Case 2: $u \equiv 3 \bmod 4$.

Assume $t = 2^e u$ is a sum of two squares in $\mathbf{Z}_2$. Since $1/2 = 1/4 + 1/4$ is a sum of two squares in $\mathbf{Q}$, $u = t(1/2)^e$ is a sum of two squares in $\mathbf{Q}_2$. We will now show a 2-adic integer that is 3 mod 4 can't be a sum of two squares in $\mathbf{Q}_2$, so we get a contradiction.

Suppose $u = x^2+y^2$ in $\mathbf{Q}_2$. If x and y are both 2-adic integers then $u \equiv x^2+y^2 \bmod 4$; the only squares mod 4 are 0 and 1, whose sum two at a time can be $0, 1$, or $2 \bmod 4$, but not $3 \bmod 4$. Therefore x or y is not in $\mathbf{Z}_2$. Without loss of generality $x \notin \mathbf{Z}_2$. Then $y^2 = u - x^2$ with $|x^2|_2 = |x|_2^2 > 1 = |u|_2$, so $|y^2|_2 = |u-x^2|_2 = |x^2|_2 > 1$ by the strong triangle inequality. Set $|x|_2 = 2^n$ with $n \geq 1$, so $|y|_2 = 2^n$ too. Writing $x = v/2^n$ and $y = w/2^n$ for 2-adic units v and w, we have $v^2+w^2 = 4^n u \equiv 0 \bmod 4$. Since units square to $1 \bmod 4$ we have $v^2+w^2 \equiv 2 \bmod 4$, and that is a contradiction. □

Here is Theorem 2.1 in terms of p-adic numbers.

Theorem 2.6. *A nonzero integer is a sum of two squares in $\mathbf{Z}$ if and only if it is a sum of two squares in $\mathbf{R}$ and in every $\mathbf{Z}_p$.*

Proof. An integer that is a sum of two squares in $\mathbf{Z}$ is obviously a sum of two squares in $\mathbf{R}$ and in every $\mathbf{Z}_p$.

Conversely, assume a nonzero integer m is a sum of two squares in $\mathbf{R}$ and in every $\mathbf{Z}_p$. For a prime p dividing m with $p \equiv 3 \bmod 4$, its multiplicity $\mathrm{ord}_p(m)$ is even by Theorem 2.4. Since m is assumed to be a sum of two squares in $\mathbf{R}$ we have $m > 0$. Then Theorem 2.1 implies m is a sum of two squares in $\mathbf{Z}$. □

This proof of Theorem 2.6 made no use of Theorems 2.3 ($p \equiv 1 \bmod 4$) or 2.5 ($p = 2$). We could have dropped the use of $\mathbf{R}$ in Theorem 2.6 by looking instead at m in $\mathbf{Z}_2$: once we know $\mathrm{ord}_p(m)$ is even for primes p dividing m that are $3 \bmod 4$, so the p-power in m is a power of p^2, which is $\equiv 1 \bmod 4$, we see that each odd prime power dividing m is $1 \bmod 4$, so $m = \pm 2^e m'$ where $m' \equiv 1 \bmod 4$. Theorem 2.5 then implies $\pm m' \equiv 1 \bmod 4$, so the $\pm$ sign has to be $+$.

[2] Here is a proof by contradiction: if $-1 \equiv s^2 \bmod p$ then raising both sides to the $(p-1)/2$ power we get $(-1)^{(p-1)/2} \equiv s^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem, and also $(p-1)/2$ is odd since $p \equiv 3 \bmod 4$, so $(-1)^{(p-1)/2} = -1$. Thus $-1 \equiv 1 \bmod p$, a contradiction.

3. The Local–Global Principle for quadratic forms

If we consider quadratic forms $Q(x,y) = ax^2 + by^2$ with $a, b \in \mathbf{Z} - \{0\}$, not just $x^2 + y^2$, it is not true that being able to solve $Q(x,y) = m$ in $\mathbf{R}$ and each $\mathbf{Z}_p$ implies there is a solution in $\mathbf{Z}$.

Example 3.1. Consider $x^2 + 11y^2 = 3$. It obviously has no integer solutions, but has a solution in $\mathbf{R}$ and each $\mathbf{Z}_p$. Solvability in $\mathbf{R}$ is clear, and solvability in $\mathbf{Z}_p$ for $p \neq 2$ or 11 follows from solving the congruence $x^2 \equiv 3 - 11y^2 \bmod p$ using the pigeonhole principle (as in the proof of Theorem 2.4) and then applying Hensel's lemma.

To prove solvability in $\mathbf{Z}_2$, from $3/11 \equiv 1 \bmod 8$ we see that $3/11$ is a square in $\mathbf{Z}_2$, so we can solve $0^2 + 11y^2 = 3$ in $\mathbf{Z}_2$.

In $\mathbf{Z}_{11}$, since $3 \equiv 5^2 \bmod 11$ we can solve $x^2 + 11 \cdot 0^2 = 3$ in $\mathbf{Z}_{11}$.

Example 3.2. Consider $2x^2 + 7y^2 = 1$. There are no integer solutions, but there is a real solution and there is a solution in $\mathbf{Z}_p$ for $p \neq 2$ or 7 by solving the congruence $2x^2 \equiv 1 - 7y^2 \bmod p$ with the pigeonhole principle and then using Hensel's lemma.

In $\mathbf{Z}_2$ with $x = 1$ the equation becomes $y^2 = -1/7$, which has a 2-adic solution since $-1/7 \equiv 1 \bmod 8$.

In $\mathbf{Z}_7$ we can solve $2x^2 = 1$ by Hensel's lemma since $1/2 \equiv 4 \bmod 7$.

Using reduction and the Chinese remainder theorem, a polynomial equation with integer coefficients that has solutions in $\mathbf{Z}_p$ for all p has a solution as a congruence mod m for all $m \geq 2$: $x^2 + 11y^2 \equiv 3 \bmod m$ and $2x^2 + 7y^2 \equiv 1 \bmod m$ are both solvable for all m. Thus we see that being able to solve a polynomial equation as a congruence in every modulus does not imply (in general) that we can find a solution to the polynomial equation in $\mathbf{Z}$.

While the equations in the previous two examples lack integer solutions, they both have rational solutions. For example, $x^2 + 11y^2 = 3$ has solutions $(1/2, 1/2)$ and $(4/3, 1/3)$ and $2x^2 + 7y^2 = 1$ has solutions $(1/3, 1/3)$ and $(3/5, 1/5)$. This is a clue that solutions in $\mathbf{Q}$ and $\mathbf{Q}_p$ might be a more robust concept than solutions in $\mathbf{Z}$ and $\mathbf{Z}_p$, and this turns out to be the case.

Theorem 3.3 (Hasse–Minkowski)**.** *Let $Q(x_1, \ldots, x_n)$ be a quadratic form with rational coefficients.*

1) *For $c \in \mathbf{Q}^\times$ the equation $Q(\mathbf{x}) = c$ has a solution in $\mathbf{Q}$ if and only if it has a solution in $\mathbf{R}$ and every $\mathbf{Q}_p$.*
2) *The equation $Q(\mathbf{x}) = 0$ has a solution in $\mathbf{Q}$ besides $(0, \ldots, 0)$ if and only if it has a solution in $\mathbf{R}$ and every $\mathbf{Q}_p$ besides $(0, \ldots, 0)$.*

Moreover, in both cases when $n \geq 2$, the solvability in $\mathbf{Q}_p$ is automatic unless $p = 2$ or some coefficient[3] of $Q(\mathbf{x})$ is not in $\mathbf{Z}_p^\times$.

The point of the last part of the Hasse–Minkowski theorem is that solvability in $\mathbf{R}$ and every $\mathbf{Q}_p$ actually does not involve an infinite set of completions, but only finitely many: $\mathbf{R}$, $\mathbf{Q}_2$, and $\mathbf{Q}_p$ for the odd primes p dividing a numerator or denominator of a coefficient of $Q(\mathbf{x})$.

The significance of reducing the task of solving an equation in rational numbers to solving it in real and p-adic numbers instead (where the solutions in different completions need not have any *a priori* connection to each other) is that it is much easier to determine if a

[3]This is actually correct only if Q is in diagonal form: $Q = a_1x_1^2 + \cdots + a_nx_n^2$, with no mixed terms. Every quadratic form with rational coefficients can be put into diagonal form by a linear change of variables.

polynomial equation has a solution in a complete field than in a field like $\mathbf{Q}$: an approximate solution can often be refined to an exact solution using limits. For example, the equation $x^2 + y^2 - z^2 = c$ clearly has a real solution for every $c \in \mathbf{Q}^\times$ because we see both plus and minus signs. The condition for a quadratic form equation over $\mathbf{Q}_p$ to be solvable in $\mathbf{Q}_p$ is a bit harder than checking signs of coefficients, but it is algorithmic and can be found in detailed treatments of the Hasse–Minkowski theorem. (See [5].)

4. Counterexamples

If we move beyond quadratic forms, which have degree 2, to polynomial equations of degree 3 or higher, then we find more counterexamples to the local-global principle for $\mathbf{Z}$-solutions as we saw in Examples 3.1 and 3.2 and also even counterexamples to the local–global principle for $\mathbf{Q}$-solutions.

Example 4.1. The equation $y^2 = x^3 - 51$ has the rational solution $(1375/9, 50986/27)$, which is a solution in $\mathbf{Z}_p$ for $p \neq 3$. At $p = 3$ set $x = 1$ to make the equation $y^2 = -50$, which has a solution in $\mathbf{Z}_3$ since $-50 \equiv 1 \bmod 3$. Therefore the equation $y^2 = x^3 - 51$ has a solution in $\mathbf{R}$ (obviously) and in each $\mathbf{Z}_p$,[4] but by methods of algebraic number theory or elliptic curves it can be shown this equation has no solution in integers.

Example 4.2. Here is a famous example of Selmer [9]: the cubic equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution other than $(0, 0, 0)$ in $\mathbf{R}$ and in each $\mathbf{Q}_p$, but it has no solution in $\mathbf{Q}$ other than $(0, 0, 0)$.

There is obviously a nonzero solution in $\mathbf{R}$. To show there is a solution besides $(0, 0, 0)$ in each $\mathbf{Q}_p$ we follow a method I learned from Kevin Buzzard. The basic idea is to show there is a nonzero solution modulo p and then lift that solution p-adically by Hensel's lemma. We will separately treat the cases $p = 3$, $p = 5$, and $p \neq 3$ or 5.

To find a 3-adic solution, set $x = 0$ and $z = -1$, making the equation $4y^3 - 5 = 0$, or $y^3 = 5/4$. Although $5/4 \equiv -1 \bmod 9$ and -1 is a 3-adic cube, this congruence isn't sharp enough to conclude with Hensel's lemma that $5/4$ is a 3-adic cube: to use Hensel's lemma we seek a $\beta \in \mathbf{Z}_3^\times$ such that $|\beta^3 - 5/4|_3 < 1/9$, i.e., $\beta^3 \equiv 5/4 \equiv 8 \bmod 27$. The choice $\beta = 2$ works, so $5/4$ is a 3-adic cube and we can solve Selmer's equation in $\mathbf{Q}_3$ as $(0, y, -1)$ where $y^3 = 5/4$ in $\mathbf{Z}_3$.

If $p \neq 3$ and a is a nonzero cube mod p then a is a cube in $\mathbf{Z}_p^\times$ by Hensel's lemma for $X^3 - a$. In particular, for $p = 5$, set $x = 1$ and $z = 0$ to make Selmer's equation $3 + 4y^3 = 0$, or $y^3 = -3/4$. Since $-3/4 \equiv 3 \equiv 2^3 \bmod 5$, by Hensel's lemma for $X^3 + 3/4$ with approximate solution 2 we see that $-3/4$ is a 5-adic cube. We get a 5-adic solution to Selmer's equation as $(1, y, 0)$ where $y^3 = -3/4$ in $\mathbf{Z}_5$.

From now on let p be a prime other than 3 or 5 (this includes allowing $p = 2$). Then $3, 5 \not\equiv 0 \bmod p$. We are going to look at the group $(\mathbf{Z}/(p))^\times$, which is *cyclic* of order $p - 1$. What proportion of the group is filled up by cubes?

- If $p \equiv 1 \bmod 3$ then the cubes in $(\mathbf{Z}/(p))^\times$ are a subgroup of index 3.
- If $p \not\equiv 1 \bmod 3$ then $(3, p - 1) = 1$, so every number in $(\mathbf{Z}/(p))^\times$ is a cube.

If 3 mod p is a cube then 3 is a cube in $\mathbf{Z}_p$ by Hensel's lemma for $X^3 - 3$, so we can solve Selmer's equation as $(x, 1, -1)$ where $x^3 = 1/3$ in $\mathbf{Q}_p$.

[4]More generally, for every integer k the equation $y^2 = x^3 + k$ has a solution in $\mathbf{R}$ and in every $\mathbf{Z}_p$.

If 3 mod p is not a cube then not all numbers in $(\mathbf{Z}/(p))^\times$ are cubes. Thus $p \equiv 1 \bmod 3$, so the nonzero cubes mod p are a subgroup of $(\mathbf{Z}/(p))^\times$ that has index 3 and coset representatives $\{1, 3, 9\}$: for every $a \not\equiv 0 \bmod p$ we have $a \equiv b^3, 3b^3$, or $9b^3 \bmod p$ for some $b \not\equiv 0 \bmod p$. We will apply this with $a = 5$.

- If $5 \equiv b^3 \bmod p$ then 5 is a cube in $\mathbf{Z}_p$ by Hensel's lemma for $X^3 - 5$, and we can solve Selmer's equation as $(-y, y, -1)$ where $y^3 = 5$ in $\mathbf{Z}_p$.
- If $5 \equiv 3b^3 \bmod p$ then $5/3$ is a cube in $\mathbf{Z}_p$ by Hensel's lemma and we can solve Selmer's equation as $(x, 0, -1)$ where $x^3 = 5/3$.
- If $5 \equiv 9b^3 \bmod p$ then $5 \cdot 3 = 15$ is a cube in $\mathbf{Z}_p$ by Hensel's lemma and we can solve Selmer's equation as $(3t, 5, -7)$ where $t^3 = 15$. That is, $3a^3 + 4b^3 = 5c^3$ where $a = 3t$, $b = 5$, and $c = 7$.

This completes the proof that Selmer's equation has local solutions everywhere. That the equation has no rational solution besides $(0, 0, 0)$ is harder. There are proofs using algebraic number theory [4] or elliptic curves [3, pp. 86–87].

Even though the local–global principle for cubic equations is not always true, one of the most important unsolved problems in mathematics – the Birch and Swinenrton-Dyer conjecture – is a relationship between the behavior of rational solutions and the real and p-adic solutions of cubic equations (elliptic curves).

5. Local–global principle for powers

We start with a simple example of how the local–global principle manifests itself for powers of rational numbers.

Theorem 5.1. *A rational number is an nth power in $\mathbf{Q}$ if and only if it is an nth power in $\mathbf{R}$ and every $\mathbf{Q}_p$.*

Proof. The "only if" direction is clear. Assume now that $r \in \mathbf{Q}$ and we can solve $x^n = r$ in $\mathbf{R}$ and in each $\mathbf{Q}_p$. To prove r is an nth power in $\mathbf{Q}$ we can assume $r \neq 0$.

For each prime p appearing in r (in either the numerator or denominator), the assumption that r is an nth power in $\mathbf{Q}_p$ implies $\mathrm{ord}_p(r)$ is divisible by n. Therefore every prime appearing in r shows up within an nth power, so $r = \pm s^n$ for some $s \in \mathbf{Q}$. If n is odd then we can absorb the sign into s and r is an nth power in $\mathbf{Q}$. if n is even then the fact that r is an nth power in $\mathbf{R}$ forces $r > 0$, so $r = s^n$ is again an nth power in $\mathbf{Q}$. □

This theorem was not hard to prove, but it has refinements that lie deeper. For example, when $n = 2$ there is a local–global theorem for rational squares that allows any finite number of completions to be removed without changing the conclusion: if $r \in \mathbf{Q}^\times$ and r is a square in all but at most finitely many completions from $\mathbf{R}$ and each $\mathbf{Q}_p$ then in fact $r = s^2$ for some $s \in \mathbf{Q}^\times$. Since the proof of Theorem 5.1 was based on looking in $\mathbf{Q}_p$ for each p dividing the numerator or denominator of r, proving Theorem 5.1 without having each $\mathbf{Q}_p$ available is a challenge. As an example, how could we prove -2 is not a square in $\mathbf{Q}$ from local considerations if we are not allowed to work in $\mathbf{R}$ and $\mathbf{Q}_2$? We could do this by working in $\mathbf{Q}_5$ since -2 is not a square there (because $-2 \bmod 5$ is not a square), and if we are not allowed to work in $\mathbf{Q}_5$ either then we could work in $\mathbf{Q}_7$ (where -2 is not a square). More generally, it can be shown from the quadratic reciprocity law in number theory that -2 is not a square in $\mathbf{Q}_p$ if $p \equiv 5, 7 \bmod 8$ and also that there are infinitely many primes satisfying each of those congruence conditions, so we can always show -2 is not a square using local considerations if any finite number of completions is removed.

Theorem 5.1 with finitely many completions removed works not just for $n = 2$, but for all n up to 7. That is, if $2 \leq n \leq 7$ then the nth powers in $\mathbf{Q}^\times$ are precisely the nonzero rational numbers that are nth powers in all but finitely many completions of $\mathbf{Q}$. However, when $n = 8$ the pattern breaks: being an 8th power in all but at most finitely many completions of $\mathbf{Q}$ need not imply being an 8th power in $\mathbf{Q}$.

Example 5.2. We show 16 is an 8th power in every completion of $\mathbf{Q}$ except $\mathbf{Q}_2$. Write

$$X^8 - 16 = (X^4 - 4)(X^4 + 4) = (X^2 - 2)(X^2 + 2)(X^2 + 2X + 2)(X^2 - 2X + 2).$$

The two quadratic factors both have discriminant -4, so there is an 8th root of 16 in a completion of $\mathbf{Q}$ as long as that completion contains a square root of 2 or -2 or -4.

Clearly 2 is a square in $\mathbf{R}$. For each odd prime p, one of the numbers 2, -2, or -4 is a square in $(\mathbf{Z}/(p))^\times$ (more generally, if $a, b \not\equiv 0 \bmod p$ then a, b, or ab is a square in $(\mathbf{Z}/(p))^\times$ – this is because the squares in $(\mathbf{Z}/(p))^\times$ are a subgroup of index 2), so 2, -2, or -4 is a square in $\mathbf{Q}_p$ by Hensel's lemma. Therefore 16 an 8th power in every completion of $\mathbf{Q}$ other than $\mathbf{Q}_2$, where it obviously is not since $\mathrm{ord}_2(16)$ is not a multiple of 8.

A similar example occurs for each n divisible by 8 (and not for any other n): $2^{n/2}$ is an nth power in each $\mathbf{Q}_p$ and $\mathbf{R}$ except for $\mathbf{Q}_2$. Indeed, in each of those fields we can write $16 = x^8$ so $2^{n/2} = 16^{n/8} = x^n$. Here is a version of this story using just modular arithmetic rather than anything p-adic.

Theorem 5.3. *For $a \in \mathbf{Z}$, if $x^n \equiv a \bmod p$ is solvable for all but finitely many primes p then $a = b^n$ for some $b \in \mathbf{Z}$ if $8 \nmid n$, and a is either b^n or $2^{n/2}b^n$ for some $b \in \mathbf{Z}$ if $8 \mid n$.*

When $p \nmid n$ and $p \nmid a$, solvability of the mod p congruence $x^n \equiv a \bmod p$ in $\mathbf{Z}/(p)$ and solvability of the equation $x^n = a$ in $\mathbf{Z}_p$ are equivalent by Hensel's lemma.

Theorem 5.3 was first proved by Trost [11] in 1934.[5] Nobody noticed and the theorem was rediscovered by Ankeny and Rogers [1] in 1951. The criterion describing when a nonzero number in $\mathbf{Q}$ or any finite extension of $\mathbf{Q}$ is an nth power if it is an nth power in all but finitely many completions is called the Grunwald–Wang Theorem [14]. It was originally just Grunwald's theorem (1933), with no exceptional case recognized when $8 \mid n$, until Wang [12] found a counterexample to it 15 years after Grunwald's paper appeared [6] and 6 years after Whaples [13] had published a *second* proof of Grunwald's incorrect theorem. The setting in which Wang worked was sufficiently technical that the very simple form of Example 5.2 as a counterexample was not noticed for a while. That is probably how [1] could appear a few years after [12] in the same journal with no mention of their connection or the link to [11].

6. Local-global principle for heights

In number theory, a useful way to measure the computational complexity of a rational number r is by the size of its numerator and denominator when r is written in reduced form: if $r = a/b$ where a and b are relatively prime integers, we set the *height* of r to be

$$H(r) = \max(|a|, |b|). \tag{6.1}$$

(The numerator and denominator in reduced form are only defined up to scaling by -1, but this ambiguity does not affect the value of the height.) For example, $H(0) = \max(0, 1) = 1$, $H(2/3) = 3$, and $H(-9/6) = H(-3/2) = 3$. The height is always a positive integer, so $H(r) \geq 1$. While there are infinitely many rational numbers with ordinary absolute value

[5]For prime n, a proof of Trost's theorem is in [7, pp. 57–58] for $n = 2$ and [7, pp. 220-221] for $n \neq 2$.

up to a given bound, there are only finitely many rational numbers having height up to a given bound.[6] This makes the height a useful means of counting rational numbers.

The formula (6.1) is biased towards the archimedean absolute value on $\mathbf{Q}$. There turns out to be an alternate formula for the height with two benefits: all the absolute values on $\mathbf{Q}$ participate on an equal footing and the formula does not require r to be written in reduced form. We present it in Theorem 6.2 below after a brief but important lemma.

Lemma 6.1 (Product formula)**.** *For $r \in \mathbf{Q}^\times$, $\prod_v |r|_v = 1$, where v runs over primes and ∞, with $|\cdot|_\infty$ being the archimedean absolute value on $\mathbf{Q}$.*

Proof. Since $|r|_p = 1$ when p does not divide the numerator or denominator of r, the product $\prod_v |r|_v$ has only finitely many terms in it that might not be 1. Writing $r = a/b$ for nonzero integers a and b, we have $\prod_v |r|_v = (\prod_v |a|_v)/(\prod_v |b|_v)$, so it suffices to prove the lemma when $r = a$ is an integer. If $a = \pm 1$ then $\prod_v |a|_v = 1$ since each $|a|_v$ is 1. Otherwise write a by its prime factorization: $a = \pm p_1^{e_1} \cdots p_k^{e_k}$ where the p_i are distinct primes. Then $|a|_\infty = p_1^{e_1} \cdots p_k^{e_k}$, $|a|_{p_i} = 1/p_i^{e_i}$, and $|a|_p = 1$ if $p \notin \{p_1, \ldots, p_k\}$, so

$$\prod_v |a|_v = |a|_\infty |a|_{p_1} \cdots |a|_{p_k} = p_1^{e_1} \cdots p_k^{e_k} \frac{1}{p_1^{e_1}} \cdots \frac{1}{p_k^{e_k}} = 1.$$

□

The product formula seems innocuous, but it is a fundamental result gluing together all the different absolute values of $\mathbf{Q}$ and can in fact be taken as a starting point for algebraic number theory [2].

Theorem 6.2. *Let $r \in \mathbf{Q}$ be rational. Then*

$$H(r) = \prod_v \max(|r|_v, 1),$$

where the product runs over all absolute values of $\mathbf{Q}$.[7]

Example 6.3. If $r = 3/2$ then $|r|_v = 1$ for $v \notin \{\infty, 2, 3\}$ and

$$\prod_v \max(|r|_v, 1) = \max(|r|_\infty, 1) \max(|r|_2, 1) \max(|r|_3, 1) = \frac{3}{2} \cdot 2 \cdot 1 = 3 = H(r).$$

If $r = 2/3$ then

$$\prod_v \max(|r|_v, 1) = \max(|r|_\infty, 1) \max(|r|_2, 1) \max(|r|_3, 1) = 1 \cdot 1 \cdot 3 = 3 = H(r).$$

Proof. In the product $\prod_v \max(|r|_v, 1)$ only finitely many factors are not 1 since that is true about $|r|_v$. Therefore this infinite product is really just a finite product, with the terms not equal to 1 depending on r.

Let the reduced form of r be a/b. Then

$$\prod_v \max(|r|_v, 1) = \prod_v \max\left(\left|\frac{a}{b}\right|_v, 1\right).$$

[6] Explicitly, $|\{r \in \mathbf{Q} : H(r) \leq x\}| = (12/\pi^2)x^2 + O(x \log x)$ as $x \to \infty$.

[7] Strictly speaking we should say something like all "normalized" absolute values of $\mathbf{Q}$, since $\sqrt{|\cdot|_\infty}$ and $|\cdot|_7^3$ are also absolute values. We are using a set of absolute values on $\mathbf{Q}$ that fit together into the product formula.

Multiplying this by 1 in the form $\prod_v |b|_v$, from the product formula, we get

$$\prod_v \max\left(\left|\frac{a}{b}\right|_v, 1\right) = \prod_v |b|_v \prod_v \max\left(\frac{|a|_v}{|b|_v}, 1\right) = \prod_v |b|_v \max\left(\frac{|a|_v}{|b|_v}, 1\right) = \prod_v \max\left(|a|_v, |b|_v\right)$$

and now we use the fact that a and b are relatively prime integers: for each prime p, $|a|_p \leq 1$ and $|b|_p \leq 1$, with either $|a|_p = 1$ or $|b|_p = 1$ because p can't divide both a and b. Thus $\max(|a|_p, |b|_p) = 1$ for all p, so

$$\prod_v \max\left(|a|_v, |b|_v\right) = \max(|a|_\infty, |b|_\infty),$$

which by definition is the height of r. □

More generally, for $n \geq 1$ and rational numbers $r_0, \ldots, r_n$ that are not all 0 we have

$$\prod_v \max(|r_0|_v, \ldots, |r_n|_v) = \max(|a_0|_\infty, \ldots, |a_n|_\infty) \tag{6.2}$$

where $a_0, \ldots, a_n$ are the numerators of the r_i's when we write them with a least common denominator d: $r_i = a_i/d$ for all i. (Necessarily the numerators $a_0, \ldots, a_n$ are relatively prime as an n-tuple, since otherwise d would not be a least common denominator.) When $n = 1$, $r_0 = r$, and $r_1 = 1$ we recover Theorem 6.2 from (6.2) since $r = a/b$ and $1 = b/b$ is the representation of r and 1 with least common denominator when a/b is the reduced form of r.

If we replace r_i in (6.2) with sr_i for some common factor $s \in \mathbf{Q}^\times$ then the left side of (6.2) is unchanged by the product formula ($\prod_v |s|_v = 1$). This makes (6.2) the starting point for the study of heights on projective n-space over $\mathbf{Q}$.

References

[1] N. C. Ankeny and C. A. Rogers, *A Conjecture of Chowla*, Annals of Math. **53** (1951), 541–550.
[2] E. Artin and G. Whaples, *Axiomatic Characterization of Fields by the Product Formula for Valuations*, Bull. Amer. Math. Soc. **51** (1945), 469–492.
[3] J. W. S. Cassels, "Lectures on Elliptic Curves," Cambridge Univ. Press, Cambridge, 1991.
[4] K. Conrad, Selmer's Example, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/selmerexample.pdf.
[5] A. Gamzon, The Hasse–Minkowski Theorem, UConn Honors Thesis, 2006. Online at http://digitalcommons.uconn.edu/srhonors_theses/17/.
[6] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, J. reine angew. Math. **169** (1933), 103–107.
[7] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer, 1990.
[8] P. Roquette, In Memoriam Ernst Steinitz, http://www.rzuser.uni-heidelberg.de/~ci3/STEINITZ.pdf.
[9] E. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Arithmetica **85** (1951), 203–362.
[10] E. Steinitz, *Algebraische Theorie der Körper*, J. reine angew. Math. **137** (1910), 167-309
[11] E. Trost, *Zur Theorie der Potenzreste*, Nieuw Arch. Wisk. **18** (1934), 58–61.
[12] S. Wang, *A Counter-Example to Grunwald's Theorem*, Annals of Math. **49** (1948), 1008–1009.
[13] G. Whaples, *Non-analytic class field theory and Grunwald's theorem*, Duke Math. J. **9** (1942), 455–473.
[14] Wikipedia, Grunwald–Wang Theorem, https://en.wikipedia.org/wiki/Grunwald-Wang_theorem.