THE CONGRUENCE SUBGROUP PROBLEM FOR UNITS

KEITH CONRAD

Let K be a number field. Denote the unit group of $\mathcal{O}_K$ by U_K. For any nonzero ideal $\mathfrak{c}$ in $\mathcal{O}_K$, let

$$U_K(\mathfrak{c}) = \{u \in U_K : u \equiv 1 \bmod \mathfrak{c}\}.$$

This is the kernel of $U_K \to (\mathcal{O}_K/\mathfrak{c})^\times$.

A subgroup of U_K that contains $U_K(\mathfrak{c})$ for some $\mathfrak{c}$ is called a *congruence subgroup*. For a subgroup $\Gamma \subset U_K$ that contains $U_K(\mathfrak{c})$, any $u \in U_K$ that is congruent mod $\mathfrak{c}$ to an element of Γ has to lie in Γ. Therefore Γ can be defined by congruence conditions, simply by indicating which congruence classes Γ consists of in the finite group $(\mathcal{O}_K/\mathfrak{c})^\times$ when we reduce Γ modulo $\mathfrak{c}$. This explains the terminology "congruence subgroup."

Being the kernel of a homomorphism from U_K into a finite group, $U_K(\mathfrak{c})$ has finite index in U_K. Therefore any congruence subgroup of U_K has finite index. Whether or not the converse holds is called the congruence subgroup problem: if $\Gamma \subset U_K$ is a finite index subgroup, does Γ contain $U_K(\mathfrak{c})$ for some nonzero ideal $\mathfrak{c}$?

For example, the units in $\mathbf{Z}[\sqrt{2}]$ are $\pm(1+\sqrt{2})^{\mathbf{Z}}$. The subgroup of positive units has index 2. Is there a nonzero $\alpha \in \mathbf{Z}[\sqrt{2}]$ such that any *unit* in $\mathbf{Z}[\sqrt{2}]$ satisfying $u \equiv 1 \bmod \alpha$ is positive? (Every congruence class in every $\mathbf{Z}[\sqrt{2}]/\alpha$, $\alpha \neq 0$, contains both positive and negative numbers; add and subtract α enough times from any number. So a congruence condition can't force a sign condition on unrestricted elements of $\mathbf{Z}[\sqrt{2}]$. However, our elements are restricted: we're looking only at *units*.) As another example, the squared units in $\mathbf{Z}[\sqrt{2}]$ are a subgroup of index 4 in all units. Can a congruence condition on units in $\mathbf{Z}[\sqrt{2}]$ force them to be squares?

Theorem 1 (Chevalley, 1951)**.** *For any number field K, every subgroup of finite index in U_K is a congruence subgroup. In other words, the congruence subgroup problem has an affirmative answer for U_K.*

To prove Chevalley's theorem we need three preliminary results. The first two are algebraic and the third is arithmetic.

Lemma 2. *Let p be a prime, K any field of characteristic not equal to p, and r a positive integer. Any element of K that is a p^rth power in $K(\zeta_{p^r})$ is a p^rth power in K, with the proviso that $i = \sqrt{-1}$ is in K if $p = 2$.*

Proof. This is due to Chevalley. See the remark after the proof of [1, Théorème 1], and items 2, 3, 4, and 5 in that proof. (Warning: the second proof of that theorem is incorrect.) ☐

The case $p = 2$ in Lemma 2 requires that extra condition about i, since $-4 = (1+i)^4$ is a fourth power in $\mathbf{Q}(i) = \mathbf{Q}(\zeta_4)$ but not in $\mathbf{Q}$.

Lemma 3. *Let K be a field with characteristic not equal to 2 and $i \notin K$. Choose $k \geq 2$ maximal such that $\zeta_{2^k} \in K(i)$. For any $e \geq 0$, if $x \in K$ is a 2^{k+e}th power in $K(i)$, then x is a 2^eth power in K.*

Proof. See Chevalley [1, p. 37]. □

Lemma 4. *If $F \subset L$ and all but finitely many primes in F split completely in L, then $L = F$.*

Proof. The shortest argument uses analytic properties of zeta-functions of number fields. The hypothesis implies that $\zeta_L(s)$ is equal to $\zeta_F(s)^{[L:F]}$ up to multiplication by finitely many Euler factors. Computing pole orders at $s = 1$ shows $1 = [L : F]$, so $L = F$. □

We now turn to a proof of Chevalley's theorem (following Chevalley).

Proof. Let $\Gamma \subset U_K$ have finite index, say m. Since U_K/Γ has order m, $U_K^m \subset \Gamma$, where U_K^m is the group of mth powers of units. Because U_K is finitely generated, U_K^m has finite index in U_K. Therefore it suffices to verify U_K^m is a congruence subgroup of U_K for every m and every K.

Step 1: Reduction to prime power m and $\zeta_m \in K$

Since the intersection of two congruence subgroups is a congruence subgroup (exercise), and $U_K^m \cap U_K^{m'} = U_K^{mm'}$ for relatively prime m and m', it suffices to consider the case when m is a prime power. Prime power exponents are convenient because of Lemma 2, which will let us reduce to the case when K contains suitable roots of unity. (This is how Chevalley was led to Lemma 2.)

Let m be a prime power and K be any number field. We show there is an integer $n \geq 1$ such that

$$U_K^m = U_{K(\zeta_n)}^n \cap U_K. \tag{1}$$

If m is an odd prime power, or if m is a power of 2 and $i \in K$, then we can let $n = m$ by Lemma 2. (Powers and roots of units are again units, so Lemma 2 with K a number field remains valid when fields are replaced by unit groups.)

What if m is a power of 2 and $i \notin K$? Is (1) true with $n = m$? When $m = 2$, $K(\zeta_m) = K$ and we can use $n = 2$ in (1). But we can't always take $n = 4$ when $m = 4$ (exercise). For this we use Lemma 2.

If $m = 2^e$ and $i \notin K$ then successive applications of Lemma 2 (with $K(i)$ as base field) and Lemma 3 show we can take $n = 2^k m = 2^{k+e}$ in (1), where k comes from Lemma 3.

If $U_{K(\zeta_n)}^n$ is a congruence subgroup of $U_{K(\zeta_n)}$, (1) implies U_K^m is a congruence subgroup of U_K. Writing $K(\zeta_n)$ as K, we have reduced to the following:

Step 2: Show U_K^n is congruence subgroup of U_K when $\zeta_n \in K$, n a prime power.

Let $n = p^e$ be any prime power and K be a number field containing the nth roots of unity. We want to find a nonzero ideal $\mathfrak{c}$ in $\mathcal{O}_K$ such that any *unit* satisfying $u \equiv 1 \bmod \mathfrak{c}$ is a p^eth power. The argument will use Kummer theory.

The group U_K is finitely generated, say by $u_1, \ldots, u_t$. (At least one u_j is a root of unity, and others usually have infinite order, but we treat all generators on an equal footing.) Let $L = K(\sqrt[n]{u_1}, \ldots, \sqrt[n]{u_t})$, so L contains the nth roots of every unit in K.

Since n is a power of p, Kummer theory implies L/K is an abelian extension of p-power degree. In a finite abelian p-group (or even a finite nonabelian p-group), every proper subgroup lies in a maximal proper subgroup, which must have index p in the whole group. By Galois theory, L contains subfields $L_1, \ldots, L_s$ that have degree p over K and every intermediate field other than K contains an L_j.

For each L_j, Lemma 4 implies there are infinitely many primes in K that don't split completely in L_j. Since L_j/K is Galois of prime degree p, the only options for primes in K

that don't split completely in L_j are to ramify or to remain prime. There are only finitely many of the former, and thus infinitely many of the latter. For $j = 1, \dots, s$, let $\mathfrak{q}_j$ be a prime in K that remains prime in L_j and does not divide n.

We claim any unit $u \in U_K$ that satisfies $u \equiv 1 \bmod \mathfrak{q}_1 \cdots \mathfrak{q}_s$ is an nth power in K, and thus also in U_K. (If any $\mathfrak{q}_j$ fits more than one L_j, we only need to include it in the modulus once.) The congruence condition on u implies $X^n - u$ splits into distinct linear factors modulo each $\mathfrak{q}_j$ (because K contains the nth roots of unity). Therefore $\mathfrak{q}_j$ splits completely in $K(\sqrt[n]{u}) \subset L$. Since $\mathfrak{q}_j$ remains prime in each L_j, $K(\sqrt[n]{u})$ can't contain any L_j. That forces $K(\sqrt[n]{u}) = K$ by the definition of the L_j's, so u is an nth power in K. $\square$

The most essential property of U_K for Theorem 1 is that it's a finitely generated subgroup of $K^\times$. Chevalley [1] established Theorem 1 for all such subgroups of $K^\times$: every finite-index subgroup of a finitely generated subgroup of $K^\times$ can be defined by appropriate congruence conditions.

The congruence subgroup problem can be posed for groups defined over number fields other than unit groups. For a discussion of the congruence subgroup problem in these settings, see [3], [4], and [5].

Example 5. Taking $K = \mathbf{Q}(\sqrt{2})$, let U_K^+ be the positive units of $\mathbf{Z}[\sqrt{2}]$. This has index 2 in U_K, since $U_K = \pm U_K^+$, and $U_K^2 \subset U_K^+ \subset U_K$. To find an explicit ideal $\mathfrak{c}$ in $\mathbf{Z}[\sqrt{2}]$ such that $u \equiv 1 \bmod \mathfrak{c}$ for units u implies $u > 0$, we can work through the proof of Chevalley's theorem, which amounts to proving U_K^2 is a congruence subgroup. Since $U_K = \pm(1+\sqrt{2})^{\mathbf{Z}}$ we consider $L = K(\sqrt{-1}, \sqrt{1+\sqrt{2}})$, which is an abelian extension of degree 4. The diagram below shows the intermediate fields between L and K.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(\sqrt{-1}) \arrow[dr, dash] & K(\sqrt{1+\sqrt{2}}) \arrow[d, dash] & K(\sqrt{-1-\sqrt{2}}) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

For each of the three intermediate quadratic extensions of K we need to find a prime in $\mathbf{Z}[\sqrt{2}]$ that stays prime when extended to the quadratic extension. The prime $\mathfrak{q} = (3+\sqrt{2})$in $\mathbf{Z}[\sqrt{2}]$ has residue field of order $|\operatorname{N}(3+\sqrt{2})| = 7$ and in $\mathbf{Z}[\sqrt{2}]/\mathfrak{q} \cong \mathbf{Z}/(7)$ the number -1 is not a square and $1+\sqrt{2} \equiv -2 \equiv 5 \bmod \mathfrak{q}$, which is not a square in $\mathbf{Z}/(7)$. Thus $\mathfrak{q}$ stays prime when extended to $K(\sqrt{-1})$ and to $K(\sqrt{1+\sqrt{2}})$, but it splits when extended to $K(\sqrt{-1-\sqrt{2}})$ since $-1-\sqrt{2} \equiv 2 \equiv 9 \bmod \mathfrak{q}$.[1] For the prime $\mathfrak{q}' = (3-\sqrt{2})$, also of norm 7, we have in the residue field at $\mathfrak{q}'$ that $-1-\sqrt{2} = -4 = 3$, which is not a square in $\mathbf{Z}/(7)$. Thus, from the proof of Chevalley's theorem, we can use $\mathfrak{c} = \mathfrak{q}\mathfrak{q}' = (7)$. That is, if $\pm(1+\sqrt{2})^k \equiv 1 \bmod 7$ then the sign is $+$ and the exponent k is even.

That the modulus $\mathfrak{c} = (7)$ in $\mathbf{Z}[\sqrt{2}]$ has $U_K(\mathfrak{c}) \subset U_K^2$ can be checked directly: the order of $1+\sqrt{2} \bmod 7$ is 6, so if $(1+\sqrt{2})^k \equiv 1 \bmod 7$ then $6 \mid k$ so k is even, and $-(1+\sqrt{2})^k \not\equiv 1 \bmod 7$ for all k (check explicitly $k = 0, 1, \dots, 5$, or check fewer k if you see how to be more efficient).

[1] We can read off how the prime $\mathfrak{q}$ in K decomposes in $K(\sqrt{u})$ for any unit u from the way $X^2 - u \bmod \mathfrak{q}$ decomposes because $\mathfrak{q}$ has odd norm, whether or not the integers of $K(\sqrt{u})$ really equals $\mathcal{O}_K[\sqrt{u}]$.

Corollary 6. *For any positive integer m, the group of m-th powers U_K^m contains a subgroup $U_K(n)$ for some positive integer n :*

$$\{u \in U_K : u \equiv 1 \bmod n\} \subset U_K^m.$$

Proof. By Chevalley's theorem, there is an ideal $\mathfrak{c}$ such that $U_K(\mathfrak{c}) \subset U_K^m$. Let n be a positive integer in $\mathfrak{c}$ (*e.g.*, a generator of $\mathfrak{c} \cap \mathbf{Z}$). Then $n\mathcal{O}_K \subset \mathfrak{c}$, so $U_K(n) \subset U_K(\mathfrak{c}) \subset U_K^m$. $\square$

The modulus n in the corollary depends on m. It is conjectured that when m is a power of a prime p that we can take for n a power of p: given any p^a, there is a p^b such that

$$u \in U_K, \quad u \equiv 1 \bmod p^b \Longrightarrow u \in U_K^{p^a}. \tag{2}$$

For example, when $h(\mathbf{Q}(\zeta_p))$ is not divisible by p, Kummer's lemma says that if $K = \mathbf{Q}(\zeta_p)$ and $a = 1$ then we can choose $b = 1$: any unit in $\mathbf{Q}(\zeta_p)$ that is congruent to 1 mod $p\mathbf{Z}[\zeta_p]$ is a pth power of a unit. When K is totally real, the conjecture (2) is equivalent to Leopoldt's conjecture about the nonvanishing of the p-adic regulator of K. So we can consider (2) to be a version of Leopoldt's conjecture for all number fields. See [2] for more in this direction.

References

[1] C. Chevalley, "Deux Théorèmes d'Arithmétique," J. Math. Soc. Japan, **3** (1951), 36–44.
[2] K. Iwasawa, "A simple remark on Leopoldt's conjecture," pp. 862–870 in *Collected Papers, Vol. II*, Springer-Verlag, 2001.
[3] M. S. Raghunathan, "The congruence subgroup problem," pp. 465–494 in *Proceedings of the Hyderabad Conference on Algebraic Groups*, Manoj Prakashan, Madras, 1991.
[4] A. S. Rapinchuk, "The congruence subgroup problem," pp. 175–188 in *Algebra, K-theory, groups, and education*, Amer. Math. Soc., Providence, 1999.
[5] J-P. Serre, "Groupes de congruence (d'après H. Bass, H. Matsumoto, J. Mennicke, J. Milnor, C. Moore)," *Séminaire Bourbaki* 1966/1967, **14** (1968), W. A. Benjamin, New York, 1968. (Oeuvres II, 460–469).