The smallest prime with a given splitting type in an abelian number field

Paul Pollack

University of Georgia

January 10, 2013

Gauss's lemma (no, not that one)

Gauss's first proof of quadratic reciprocity was by induction. Playing a key role was the following remarkable result which Gauss established by an ingenious elementary argument.

Theorem (Gauss)

For every prime $p \equiv 1 \pmod 8$, then there is an odd prime $q < 1 + 2\sqrt{p}$ for which pNq – that is, p is a quadratic nonresidue modulo q.

Gauss's lemma (no, not that one)

Gauss's first proof of quadratic reciprocity was by induction. Playing a key role was the following remarkable result which Gauss established by an ingenious elementary argument.

Theorem (Gauss)

For every prime $p \equiv 1 \pmod 8$, then there is an odd prime $q < 1 + 2\sqrt{p}$ for which pNq – that is, p is a quadratic nonresidue modulo q.

In other words, the smallest rational prime q that stays inert in $\mathbb{Q}(\sqrt{p})$ is smaller than $1 + 2\sqrt{p}$.

What's your problem?

Recall that for an abelian extension $K/\mathbb{Q}$, the **conductor** is the least f for which $K \subset \mathbb{Q}(\zeta_f)$.

Gauss's problem

Let p be an odd prime. Bound from above the smallest rational prime that stays inert in the quadratic field of conductor p. (Explicitly, the field $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$.)

What's your problem?

Recall that for an abelian extension $K/\mathbb{Q}$, the **conductor** is the least f for which $K \subset \mathbb{Q}(\zeta_f)$.

Gauss's problem

Let p be an odd prime. Bound from above the smallest rational prime that stays inert in the quadratic field of conductor p. (Explicitly, the field $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$.)

Gauss's problem v2

Let χ be the quadratic Dirichlet character of conductor p. Bound from above the smallest prime q for which $\chi(q) = -1$. In fact, $\chi = \left(\frac{p^*}{\cdot}\right) = \left(\frac{\cdot}{p}\right)$ is the Legendre symbol. So we are just asking for the least prime quadratic nonresidue mod p.

Helpful: The least quad nonres mod p is automatically prime!

Character sums to the rescue!

The obvious analytic approach to v2 is to look for cancelation in the character sum

$$\sum_{n \le x} \chi(n).$$

It's enough to find an $x < p$ for which the size of the sum is smaller than the number of terms.

Indeed, in this case there is an $n \le x$ for which $\chi(n) = -1$. The least such n is the smallest (prime) quadratic nonresidue.

Character sums to the rescue!

The obvious analytic approach to v2 is to look for cancelation in the character sum

$$\sum_{n\le x}\chi(n).$$

It's enough to find an $x < p$ for which the size of the sum is smaller than the number of terms.

Indeed, in this case there is an $n \le x$ for which $\chi(n) = -1$. The least such n is the smallest (prime) quadratic nonresidue.

Pólya–I.M. Vinogradov: Cancelation occurs by $p^{1/2+\epsilon}$.
Burgess: Cancelation occurs by $p^{1/4+\epsilon}$.

(Both results give lots of cancelation, not just one.)

Vinogradov's trick

By looking at the contribution to the character sum from numbers with small prime factors, one can reduce the exponent by a factor of $1/\sqrt{e}$. This was first observed by I.M. Vinogradov, who used it in conjunction with the P–V inequality to get the exponent $1/2\sqrt{e}$.

Using the Burgess bound, one gets what is still the world record:

Theorem

The smallest prime that remains inert in the quadratic field of conductor p is $\ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.

Note: It was key that every quad. nonresidue has a prime divisor that is also a nonresidue.

A question of Linnik and A. I. Vinogradov

Problem

Let p be a prime. Give an upper bound for the least q that splits completely in $\mathbb{Q}(\sqrt{p^*})$.

Equivalently, what is the smallest prime quad. res. mod p?

A question of Linnik and A. I. Vinogradov

Problem

Let p be a prime. Give an upper bound for the least q that splits completely in $\mathbb{Q}(\sqrt{p^*})$.

Equivalently, what is the smallest prime quad. res. mod p?

Naive approach: By Linnik's theorem on primes in APs (proved twenty years before this work with Vinogradov),

$$q \ll p^L.$$

Current record: $L = 5.18$, by Xylouris
(can take $L = 4.5$ for prime moduli, a result of Meng)

A question of Linnik and A. I. Vinogradov

Problem

Let p be a prime. Give an upper bound for the least q that splits completely in the quadratic field of conductor p.

Theorem (Linnik–Vinogradov, 1966)

We have

$$q \ll_{\epsilon} p^{1/4+\epsilon}.$$

Moving on up: The smallest prime kth power residue mod p

The following generalization of the Linnik–Vinogradov theorem is due to Elliott:

Theorem

Let $K/\mathbb{Q}$ be an cyclic extension of prime conductor p and degree n, so that $D := \mathrm{Disc}(K/\mathbb{Q}) = \pm p^{n-1}$. The smallest prime q that splits completely in K satisfies

$$q \ll |D|^{1/4+\epsilon},$$

where the implied constant depends only on D and ϵ. (Note: $|D|^{1/4} = p^{(n-1)/4}$.)

Linnik/Meng gives $q \ll p^{4.5}$.
So Elliott's result is superior for small n, say $n < 19$.

The case of a general abelian number field

Theorem (P.)

Let $K/\mathbb{Q}$ be an abelian extension. Let D be the discriminant of $K/\mathbb{Q}$. The smallest rational prime q that splits completely in K satisfies

$$q \ll |D|^{1/4+\epsilon},$$

where the implied constant depends only on ϵ and the degree of $K/\mathbb{Q}$.

Again, this is superseded by Linnik's theorem on primes in APs for large degree, but sharper for small degrees.

The sketchiness... it burns!

Write $\zeta_K(s) = \sum_{n=1}^{\infty} \eta(n)/n^s$, where $\eta(n)$ is the number of integral ideals of K of norm n.

Suppose there are no split-completely primes $q \leq y$. Then $\eta(q) = 0$ for unramified $q \leq y$. By multiplicativity of η, this means η is 'almost' supported on squarefulls. We get

$$\sum_{n \leq y} \eta(n) \lessapprox y^{1/2}.$$

The sketchiness... it burns!

Write $\zeta_K(s) = \sum_{n=1}^{\infty} \eta(n)/n^s$, where $\eta(n)$ is the number of integral ideals of K of norm n.

Suppose there are no split-completely primes $q \le y$. Then $\eta(q) = 0$ for unramified $q \le y$. By multiplicativity of η, this means η is 'almost' supported on squarefulls. We get

$$\sum_{n \le y} \eta(n) \lessapprox y^{1/2}.$$

On the other hand, $\zeta_K(s)$ has a simple pole at $s = 1$, so $\sum_{n \le y} \eta(n)$ should grow linearly with y.

Since $\zeta_K(s) = \prod L(s, \chi)$, we can write η as a convolution of characters, one of which is principal. Now Burgess + Dirichlet's hyperbola method imply $y \lessapprox |D|^{1/4}$.

Getting primitive

Vinogradov–Linnik and Elliott were after the least q with $\chi(q) = 1$, where χ was a Dirichlet character of conductor p.

Let's go in the opposite direction. Let χ be an order six character mod p. What is the smallest q for which

$$\chi(q) \text{ is a primitive } 6\text{th root of unity?}$$

Otherwise asked, what is the smallest inert prime in a sextic extension of prime conductor?

Getting primitive

Vinogradov–Linnik and Elliott were after the least q with $\chi(q) = 1$, where χ was a Dirichlet character of conductor p.

Let's go in the opposite direction. Let χ be an order six character mod p. What is the smallest q for which

$$\chi(q) \text{ is a primitive } 6\text{th root of unity?}$$

Otherwise asked, what is the smallest inert prime in a sextic extension of prime conductor? Suppose that $\chi(q)$ is not a primitive 6th root of unity for $q \le y$. Then when $\chi(q) \neq 0$,

$$(1 - \chi(q)^2)(1 - \chi(q)^3) = 0.$$

Hence,

$$1 + \chi^5(q) = \chi^2(q) + \chi^3(q).$$

Getting primitive, ctd.

So for all primes $q \leq y$, we find that either $\chi(q) = 0$ or

$$1 + \chi^5(q) = \chi^2(q) + \chi^3(q).$$

Now

$$\zeta(s)L(s,\chi^5) = \prod_q \left(1 + \frac{1 + \chi^5(q)}{q^s} + \dots\right),$$

$$L(s,\chi^2)L(s,\chi^3) = \prod_q \left(1 + \frac{\chi^2 + \chi^3(q)}{q^s} + \dots\right).$$

So we suspect that if we sum the coefficients of $\zeta(s)L(s,\chi^5)$ up to y, we should get roughly the same answer as if we sum the coefficients of $L(s,\chi^2)L(s,\chi^3)$.

Getting primitive, ctd.

So for all primes $q \le y$, we find that either $\chi(q) = 0$ or

$$1 + \chi^5(q) = \chi^2(q) + \chi^3(q).$$

Now

$$\zeta(s)L(s,\chi^5) = \prod_q \left(1 + \frac{1+\chi^5(q)}{q^s} + \dots\right),$$

$$L(s,\chi^2)L(s,\chi^3) = \prod_q \left(1 + \frac{\chi^2 + \chi^3(q)}{q^s} + \dots\right).$$

So we suspect that if we sum the coefficients of $\zeta(s)L(s,\chi^5)$ up to y, we should get roughly the same answer as if we sum the coefficients of $L(s,\chi^2)L(s,\chi^3)$.

This fails once $y \gtrapprox p^{1/2}$.

Arbitrary splitting types

Theorem

Let $K/\mathbb{Q}$ be an abelian extension of degree n and conductor f. Let g be a divisor of n with $g < n$. Assume that there is at least one rational prime that does not ramify in K and that has g distinct prime ideal factors in $\mathfrak{O}_K$. Then the smallest prime q of this type satisfies

$$q \ll_{n,\epsilon} f^{\frac{n}{8}+\epsilon}.$$

Remark: We always have $f^{\frac{1}{2}[L:\mathbb{Q}]} \leq |D| \leq f^{[L:\mathbb{Q}]-1}$. So this bound is always $\lessapprox |D|^{1/4}$

Arbitrary splitting types

Theorem

Let $K/\mathbb{Q}$ be an abelian extension of degree n and conductor f. Let g be a divisor of n with $g < n$. Assume that there is at least one rational prime that does not ramify in K and that has g distinct prime ideal factors in $\mathfrak{O}_K$. Then the smallest prime q of this type satisfies

$$q \ll_{n,\epsilon} f^{\frac{n}{8}+\epsilon}.$$

Remark: We always have $f^{\frac{1}{2}[L:\mathbb{Q}]} \leq |D| \leq f^{[L:\mathbb{Q}]-1}$. So this bound is always $\lessapprox |D|^{1/4}$, hence **every splitting type** appears by going up to $\approx |D|^{1/4}$.

Thank you!