D.R. Heath-Brown
Mathematical Institute, University of Oxford
24-29 St. Giles' Oxford OX1 3LB UK
rhb@maths.ox.ac.uk

Kloosterman Centennial Celebration

Arithmetic applications of Kloosterman sums

Last April saw the 100-th anniversary of the birth of H.D. Kloosterman. The occasion was celebrated by a one day meeting in Leiden, and this article is a report on one of the lectures given. It describes one of Kloosterman's abiding contributions to mathematics, the exponential sum which now bears his name. Kloosterman sums may appear somewhat technical at first glance, but they are of frequent occurence throughout analytic number theory, and their use has brought numerous diverse applications.

H.D. Kloosterman (third from the left) in the garden of paleis Soestdijk, during the reception at the ICM in 1954.

Exponential sums are a key tool in analytic number theory. If A is a finite set of integers, and f a real valued function on A, then the sum $S = \sum_{n\in A} e^{2\pi i f(n)}$ is a typical exponential sum. Usually one writes $e(t) = \exp(2\pi i t)$, for convenience. Two types of exponential sum are commonly encountered, each handled by their own techniques. Analytic sums are those in which A is the set of integers from some finite real interval I, and f extends to a smooth function on I. Arithmetic sums are defined by giving polynomials $g(X), f(X) \in \mathbf{Z}[X]$ and a modulus $q \in \mathbf{N}$. We then take A to be the set of integers $n \in I$ for which $(h(n), q) = 1$, and set $f(n) = g(n)\overline{h(n)}/q$, where $\overline{m}$ is any integer for which $m\overline{m} \equiv 1 (\mathrm{mod}\ q)$. Thus f is, in effect, a rational function, to modulus q. In this case we have

$$S = \sum_{n\in I} e(g(n)\overline{h(n)}/q),$$

where the sum omits any values where $\overline{h(n)}$ is not defined. Notice that we get the same values for $e(g(n)\overline{h(n)}/q)$ and for S, whatever choices modulo q we make for the values of $\overline{h(n)}$.

When $h(X) = 1$ we get a sum that can be viewed either as analytic or arithmetic. Special techniques apply to such sums. The simplest example of a sum which is arithmetic but not analytic is thus

$$\sum_{n\in I} e(c\overline{n}/q) = S_I(q; c),$$

say. The usual method (often the only method) to handle arithmetic sums of this type is to convert them into sums over a 'complete' range $I = (0, q]$. This is achieved via the following result.

Lemma *Let $A_n \in \mathbf{C}$ be a sequence with period q, and let $\hat{A}_m$ be the discrete Fourier transform $\sum_{n=1}^{q} A_n e(mn/q)$. Then if $a < b$ are integers we have*

$$\left| \sum_{a<n\le b} A_n - \frac{b-a}{q}\hat{A}_0 \right| \le (\log q) \max_{1\le m<q} |\hat{A}_m|.$$

In general we expect $\hat{A}_m$ to be small for $1 \leq m < q$, so that the partial sum of the A_n is approximately described by its average value, namely $q^{-1}\hat{A}_0$.

If this lemma is applied to $S_I(q;c)$, under the assumption that I has length at most q, we find that

$$|S_I(q;c)| \leq (1+\log q) \max_{1\leq m\leq q} |S(m,c;q)|, \tag{1}$$

where

$$S(m,c;q) = \sum_{n=1}^{q} e(\frac{mn+c\overline{n}}{q}).$$

(Here again we follow the convention that values where $\overline{n}$ is not defined are omitted.) These sums $S(m,c;q)$ are the Kloosterman sums. They arise from 'completing the range' for the simplest possible genuine arithmetic exponential sum $S_I(q;c)$. Estimates for their size are crucial in bounding $S_I(q;c)$, as (1) shows.

Kloosterman's work on quadratic forms

Lagrange's famous theorem of 1770 states that every positive integer is a sum of four squares. It is natural to ask what happens if one looks at solutions of $N = a_1n_1^2 + a_2n_2^2 + a_3n_3^2 + a_4n_4^2$, with fixed coefficients $a_i \in \mathbf{N}$. Numerical experiment suggests that in some cases all integers are represented, in others all integers with a finite number of exceptions are represented, and in yet other cases infinitely many exceptions occur. In the early 1920's the Hardy-Littlewood circle method was being developed. It is a very general tool, ideally suited to investigate questions of this kind, in which one hopes to show that all integers take a certain form, with at most a finite number of exceptions. The problem above can be easily handled if one allows 5 or more variables, but for quadratic forms in 4 variables the Hardy-Littlewood method narrowly missed the target. In his seminal paper [10] in 1926, Kloosterman introduced his 'Kloosterman refinement' of the Hardy-Littlewood method. This enabled him to identify precisely which sets of coefficients a_1, a_2, a_3, a_4 allow all sufficiently large n to be represented. In his work he encountered for the first time the sums that bear his name, and succeeded in giving a non-trivial bound for them.

In the circle method one integrates a generating function around a circle, in order to pick out its coefficients by using Cauchy's integral formula. One isolates the contributions coming from the part of the circle near to each root of unity $e(n/q)$. To do this one chooses a parameter Q and arranges those fractions $n/q \in [0,1)$ for which $q \leq Q$, into increasing order. This gives a so-called 'Farey sequence'. Early applications of the circle method treated these fractions relatively crudely, but Kloosterman found it necessary to investigate their distribution fairly precisely. In particular he was interested in the length of the interval around the fraction n/q. To illustrate his argument take two consecutive Farey fractions u/v and n/q, and consider the length of the interval $[u/v, n/q]$. It is an elementary fact about such fractions that $vn - uq = 1$, so that the interval has length $1/vq$. For fractions with a fixed denominator q this varies erratically as one changes the numerator n. Indeed since $vn \equiv 1 (\mathrm{mod}\, q)$, one has $v \equiv \overline{n} (\mathrm{mod}\, q)$, so that the length of the interval $[u/v, n/q]$ is essentially determined by $\overline{n}$. However Weyl's criterion for uniform distribution shows that these lengths will be smoothly distributed, as one varies n over an interval I, providing that the sums $S_I(q;c)$ are small compared to the length of I, whenever $q \nmid c$. The key to the problem was thus to give an estimate for $S_I(q;c)$ which was substantially smaller than q.

In view of (1) one is therefore led to ask about the size of the Kloosterman sum $S(m,c;q)$. Trivially one has $|S(m,c;q)| \leq q$, but this is not quite small enough to be useful.

Kloosterman's bound

To illustrate the way in which Kloosterman found a non-trivial bound for his sum, let us consider the case in which q is a prime, p say. Then

$$S(m,c;p) = \sum_{n=1}^{p-1} e(\frac{mn+c\overline{n}}{p}),$$

where now all n in the range $1 \leq n \leq p-1$ do actually occur. Whenever a is an integer coprime to p, the residues of an run over the integers $1, \ldots, p-1$ as n does. For any such a we therefore have

$$\begin{aligned} S(m,c;p) &= \sum_{n=1}^{p-1} e(\frac{m.an + c.\overline{an}}{p}) \\ &= \sum_{n=1}^{p-1} e(\frac{ma.n + c\overline{a}.\overline{n}}{p}) \\ &= S(ma, c\overline{a}; p). \end{aligned}$$

We are assuming that $p \nmid c$, so that the values of $c\overline{a}$ are distinct for $1 \leq a \leq p-1$. The sum

$$\Sigma = \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} |S(r,s;p)|^4$$

therefore contains $p-1$ copies of $|S(m,c;p)|^4$, so that

$$(p-1)|S(m,c;p)|^4 \leq \Sigma. \tag{2}$$

We may expand $|S(r,s;p)|^4$ as

$$\sum_{n_1=1}^{p-1} \sum_{n_2=1}^{p-1} \sum_{n_3=1}^{p-1} \sum_{n_4=1}^{p-1} e(\frac{rA+sB}{p}),$$

where

$$A = n_1 + n_2 - n_3 - n_4, \quad B = \overline{n}_1 + \overline{n}_2 - \overline{n}_3 - \overline{n}_4.$$

On rearranging the orders of summation, it follows that

$$\Sigma = \sum_{n_i} \sum_{r,s} e(\frac{rA+sB}{p}) = \sum_{n_i} \{\sum_r e(\frac{rA}{p})\}\{\sum_s e(\frac{sB}{p})\}.$$

The two innermost sums are easily evaluated. If $\omega^p = 1$, but $\omega \neq 1$, then

$$\sum_{r=0}^{p-1} \omega^r = \frac{\omega^p - 1}{\omega - 1} = 0,$$

while for $\omega = 1$ the sum is plainly p. It follows that

$$\sum_{r=0}^{p-1} e(\frac{rA}{p}) = \begin{cases} 0, & p \nmid A, \\ p, & p|A, \end{cases}$$

and similarly for the sum over s. We therefore conclude that

$$\Sigma = p^2 \#\{(n_1,n_2,n_3,n_4) : p|A, B\}.$$

It is a trivial exercise to show that if $p|A, B$ then either n_3, n_4 is a permutation of n_1, n_2, or $n_1 + n_2 \equiv n_3 + n_4 \equiv 0 (\mathrm{mod}\, p)$. Thus there are at most $3(p-1)^2$ available sets of values for n_1, n_2, n_3, n_4, so that

$$\Sigma \leq 3p^2(p-1)^2 < 3p^3(p-1).$$

We now deduce from (2) that

$$|S(m,c;p)| < 3^{1/4}p^{3/4}, \quad (p \nmid c). \tag{3}$$

This is the non-trivial bound found by Kloosterman. It demonstrates that $S_I(p;c)$ contains some cancellation as soon as the length of I is of order larger than $p^{3/4}\log p$. As described above this was enough to enable Kloosterman to solve the problem on quaternary quadratic forms.

It should be mentioned that Weil [13] obtained the stronger bound

$$|S(m,c;p)| \leq 2p^{1/2}, \quad (p \nmid c) \tag{4}$$

from his proof of the Riemann Hypothesis for curves over finite fields. This estimate is essentially best possible. Many of the applications of Kloosterman sums take advantage of this stronger bound.

A recent variant of Kloosterman's problem

It is conjectured that every sufficiently large integer $N \equiv 4 (\mathrm{mod}\ 24)$ is a sum $N = p_1^2 + p_2^2 + p_3^2 + p_4^2$ with the p_i all prime. Many numbers $N \not\equiv 4 (\mathrm{mod}\ 24)$ are also of this form, but it is easy to see that one of the primes must be 2 or 3 unless $N \equiv 4 (\mathrm{mod}\ 24)$, so that the condition is needed if one is to have a problem that genuinely involves 4 variables. The analogous question with 5 primes is solved, but the case of 4 primes looks extremely difficult. An interesting approximation to the conjecture was obtained by Brüdern and Fouvry [2], using the Kloosterman refinement of the Hardy-Littlewood circle method, in conjunction with the estimate for the Kloosterman sum. They showed that every sufficiently large integer $N \equiv 4 (\mathrm{mod}\ 24)$ may be written as $N = P_1^2 + P_2^2 + P_3^2 + P_4^2$, where the P_i are 'almost-prime' in the sense that they contain only a bounded number of prime factors. To be specific they showed that one can take the P_i each to have at most 34 prime factors. This may seem a ridiculously large number, but such almost-primes have zero density in $\mathbf{N}$, so that it was quite an achievement to prove a result of this type.

An elementary problem

One apparently very elementary problem to which Kloosterman sums have been applied is the following. Let p be a prime number, and let a be an integer not divisible by p. Solve $mn \equiv a (\mathrm{mod}\ p)$ with positive integers m and n as small as possible. Write $M(a)$ for the minimal value of $\max(m,n)$. What can one say abut the size of $M(a)$? Clearly one has $M(p-1) \geq \sqrt{p-1}$, and $M(a)$ is always at most $p-1$, but is there a better upper bound? One might expect, on probabilistic grounds, that $M(a)$ is never much larger than $p^{1/2}$.

To tackle this question we shall write $A_n = 1$ if $mn \equiv a (\mathrm{mod}\ p)$ has a solution m with $1 \leq m \leq M$, say, and $A_n = 0$ otherwise. The lemma given earlier then shows that

$$\left| \sum_{0<n\leq M} A_n - \frac{M}{p}\hat{A}_0 \right| \leq (\log p) \max_{1\leq k<p} |\hat{A}_k|. \tag{5}$$

The sum $\sum_{n\leq M} A_n$ represents the number of solutions to $mn \equiv a (\mathrm{mod}\ p)$ with $1 \leq m,n \leq M$. The term $\hat{A}_0$ is just M, and

$$\hat{A}_k = \sum_{n:\exists m\leq M,\, mn\equiv a (\mathrm{mod}\ p)} e(kn/p) = \sum_{m=1}^{M} e(ka\overline{m}/p),$$

on substituting $a\overline{m}$ for n. It follows from (1) that

$$|\hat{A}_k| = |S_{(0,M]}(p,k)| \leq (1+\log p) \max_{1\leq m\leq p} |S(m,k;p)|,$$

and an application of the Weil bound (4) produces

$$|\hat{A}_k| \leq 2(1+\log p)p^{1/2}, \quad (p \nmid k).$$

Inserting this estimate into (5) shows that

$$\left| \#\{m,n \leq M : mn \equiv a (\mathrm{mod}\ p)\} - \frac{M^2}{p} \right| \leq 2(\log p)(1+\log p)p^{\frac{1}{2}} < 4(\log p)^2 p^{1/2}$$

for $p \geq 3$. Thus if $M^2/p \geq 4(\log p)^2 p^{1/2}$, we must have at least one solution to $mn \equiv a (\mathrm{mod}\ p)$ with $m,n \leq M$. We therefore deduce that

$$M(a) \leq 2(\log p)p^{3/4}.$$

This gives the desired improvement on the trivial bound $M(a) \leq p-1$. Notice that when M is appreciably larger than $p^{3/4}$, the above analysis show that there are asymptotically M^2/p solutions to $mn \equiv a (\mathrm{mod}\ p)$ with $m,n \leq M$.

It is an open problem to improve on the exponent $3/4$.

Problems involving the divisor function

The divisor function $d(n)$ is the number of divisors of n, or equivalently the number of solutions $n = ab$ with $a,b \in \mathbf{N}$. It was shown by Dirichlet that

$$\sum_{n\leq x} d(n) = x(\log x + 2\gamma - 1) + O(x^{1/2}),$$

where γ is Euler's constant. This suggests a number of problems, among them being the behaviour of $\sum_{n\leq x} d(n)d(n+1)$. This sum counts 4-tuples a,b,r,s of positive integers for which $ab \leq x$ and $ab+1 = rs$. We can eliminate s to yield the condition $ab \equiv -1 (\mathrm{mod}\ r)$. If we think of r as being fixed, and count how many solutions a,b there will be, we produce a question closely related to that of the previous section, concerning $M(-1)$. Since a and b will typically be of size $x^{1/2}$, the analysis above can be used to give an asymptotic formula for the number of pairs a,b, providing that $x^{1/2}$, which plays the rôle of M, is a little larger than $r^{3/4}$. This is satisfactory, since r is typically of size $x^{1/2}$. In this way one may obtain the asymptotic formula

$$\sum_{n\leq x} d(n)d(n+1) = xQ(\log x) + O(x^{5/6+\varepsilon}) \tag{6}$$

where ε is a small fixed positive number, and Q is a certain quadratic polynomial (whose coefficients are absolute constants that are a little unpleasant to specify).

One can replace the Weil bound by Kloosterman's bound (3) in the above analysis, in which case one will get an exponent $11/12 + \varepsilon$ in the error term. However the trivial bound $|S(m,c;p)| \leq p$ does not produce an exponent less than 1.

The sums $\sum_{n\leq x} d(n)d(n+a)$ may be handled in the same way for any $a \in \mathbf{N}$. These are of interest because they arise in the theory of the Riemann Zeta-function.

One defines, as usual

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad (s \in \mathbf{C},\ \mathrm{Re}(\mathbf{s}) > \mathbf{1}).$$

The divisor function enters via the formula $\zeta(s)^2 = \sum_{n=1}^{\infty} d(n)n^{-s}$. The mean values

$$I_k(T) = \int_0^T |\zeta(\frac{1}{2} + it)|^{2k} dt$$

have been extensively investigated. It is relatively easy to give an asymptotic formula for $I_k(T)$ for $k = 1$, while for $k \geq 3$ it is an important unsolved problem. When $k = 2$ one may write $|\zeta|^4$ as $\zeta^2\overline{\zeta^2}$. Expanding this produces a double sum whose near-diagonal terms involve $d(n)d(n+a)$, for fixed a. The analysis then reduces to a question concerning $\sum_{n \leq x} d(n)d(n+a)$. In this way Heath-Brown [5] showed that

$$\int_0^T |\zeta(\frac{1}{2} + it)|^4 dt = TF(\log T) + O(T^{7/8+\varepsilon}), \tag{7}$$

where ε is a small fixed positive number, and F is a certain quartic polynomial.

Kloostermania

In all the above problems, and many others, the key step is to use a bound on the size of the Kloosterman sum. In fact a great many of these problems involve not one, but many Kloosterman sums, occuring in various different forms of average. It was realized a long way back that if one had non-trivial estimates for averages of Kloosterman sums, then many of these results could be improved. Thus it was a major achievement when Kuznetsov [11] showed that

$$\sum_{q \leq x} \frac{S(m,n;q)}{\sqrt{q}} \ll x^{2/3+\varepsilon}$$

for any fixed small positive ε, and any fixed non-zero integers m and n. Kuznetsov's paper sparked a tremendous flurry of work, principally by Kuznetsov and Iwaniec, and their co-authors. A multitude of different kinds of averages of Kloosterman sums were investigated, and a host of applications were produced.

This activity was nicknamed 'Kloostermania', which reflected the excitement generated in the field at large. In particular it should be mentioned that the exponent $5/6$ in (6) was reduced to $2/3$ by Motohashi [12], and likewise the exponent $7/8$ in (7) was reduced to $2/3$ by Zavorotnyi [14], in both cases using the theory developed by Kuznetsov and Iwaniec.

Applications to primes

Kloostermania produced many applications to the theory of prime numbers. One such application relates to the following question. Are there infinitely many primes p such that $(p-1)/2$ is also prime? This seems to be about as hard as the twin prime conjecture. As an approximation to the problem, it was shown by Fouvry [4], that there are infinitely many p for which $(p-1)/2$ has a prime factor larger than $p^{2/3}$. Thus $(p-1)/2$ is close to being prime.

Fouvry's work itself had an interesting application. It was used by Adleman and Heath-Brown [1], in 1985, to show that the 'First Case' of Fermat's Last Theorem holds for infinitely many primes. Thus for infinitely many prime exponents p, if $x^p + y^p = z^p$, then $p|xyz$. It should be stressed that until Wiles' work, Fermat's Last Theorem was only known for finitely many primes. The above theorem of Adleman and Heath-Brown, an application of Kloosterman sums, was the only result proven to hold for infinitely many primes.

Another application of Kloostermania concerns primitive roots. If p is a prime, we say that $g \in \mathbf{Z}$ is a primitive root of p if $g + \mathbf{Z}$ generates $(\mathbf{Z}/p\mathbf{Z})^{\times}$. An equivalent statement is that the recurring expansion of $1/p$ to base g has minimal period $p-1$. It is not hard to see that 0 is never a primitive root, that -1 is a primitive root only for $p = 2$ and $p = 3$, and that a square can only be a primitive root for $p = 2$. It was conjectured by Artin that every value of g, apart from these exceptions, is a primitive root for infinitely many primes. In particular, taking $g = 10$, there should be infinitely many primes p for which the decimal expansion of $1/p$ has minimal period $p-1$.

As an approximation to Artin's conjecture one has the theorem (Heath-Brown [6]) that there are at most 2 prime values of g for which the conjecture fails; and that there are at most 3 square-free values. (Here g is said to be square-free if the only square dividing g is 1^2.) The proof uses technical results about the distribution of primes, which had previously been established using Kloostermania.

A final problem

A famous problem in prime number theory asks whether any irreducible polynomial $F(x) \in \mathbf{Z}[x]$, such that the numbers $F(1), F(2), F(3), \ldots$ have no common factor, takes infinitely many prime values. Thus for example, $n^2 + 1$ should take infinitely many prime values.

This problem appears to be well out of reach when F has degree 2 or more, so we look at an easier question, concerning the behaviour of $P(F(n))$, defined as the largest prime factor of $F(n)$, where F is assumed to have degree at least 2. It is not hard to show that $P(F(n)) \geq n$ for infinitely many n, and Nagell showed that $P(F(n))/n$ is unbounded. However it is natural to hope for stronger assertions than this.

In 1967 Hooley [8] showed, using Weil's bound (4) for the Kloosterman sum, that $P(n^2+1) \gg n^{11/10}$ infinitely often (a result subsequently improved by Deshouillers and Iwaniec [3], using Kloostermania, to allow an exponent $1.202\ldots$).

In his proof Hooley has to consider the distribution, as m varies, of the solutions of the congruence $n^2 + 1 \equiv 0 (\mathrm{mod}\ m)$. In order to show that the distribution is uniform one needs, according to the Weyl criterion, to demonstrate that the sum

$$S_1 = \sum_{m \leq x} \sum_{n:\, n^2+1 \equiv 0 (\mathrm{mod}\ m)} e(cn/m)$$

is $o(x)$. Hooley transforms this sum by setting $m = a^2 + b^2$, so that $a^2 + b^2 \equiv 0 (\mathrm{mod}\ m)$, and hence $(a\bar{b})^2 + 1 \equiv 0 (\mathrm{mod}\ m)$. Thus one can take $n = a\bar{b}$ and replace the sum S_1 by

$$S_2 = \sum_{a,b} e(\frac{ca\bar{b}}{a^2+b^2}).$$

Unfortunately this is not of the same shape as a sum $S_I(q;c)$, since the variable b appears both in the numerator and the denominator of the fraction above.

It is instructive to see how Hooley gets round this difficulty. In

general, if $u\overline{u} \equiv 1 (\mathrm{mod}\ v)$, then $u\overline{u} = 1 + vw$ for some w. Thus $vw \equiv -1 (\mathrm{mod}\ u)$, so that $w \equiv -\overline{v} (\mathrm{mod}\ u)$. In order to distinguish inverses modulo v from those modulo u we shall attach superscripts v and u as appropriate. Then we have

$$u\overline{u}^{(v)} + v(-w) = 1$$

and $-w$ is an admissible value for $v\overline{v}^{(u)}$. Thus

$$u\overline{u}^{(v)} + v\overline{v}^{(u)} = 1,$$

whence

$$\frac{\overline{u}^{(v)}}{v} + \frac{\overline{v}^{(u)}}{u} = \frac{1}{uv}.$$

We apply this with $u = b$ and $v = a^2 + b^2$. Then the term $1/uv$ is sufficiently small as to be negligible, while

$$-\frac{\overline{v}^{(u)}}{u} = -\frac{\overline{(a^2+b^2)}^{(b)}}{b} = -\frac{\overline{a^2}^{(b)}}{b}.$$

Thus

$$\frac{ca\overline{b}}{a^2+b^2}$$

may be replaced by

$$-\frac{ca\overline{a^2}^{(b)}}{b} = -\frac{c\overline{a}^{(b)}}{b}.$$

This enables us to replace S_2 by

$$\sum_b \sum_a e(-\frac{c\overline{a}^{(b)}}{b}) = \sum_b S_I(b; -c),$$

for suitable intervals $I = I(b)$.

It is now clear that we may use (1) together with the Weil bound (4) to get non-trivial bounds for S_1 and S_2, providing that the range for a is a little larger than $b^{1/2}$. This is satisfactory since a and b are typically both of size $x^{1/2}$.

Having succeeded in handling $n^2 + 1$, Hooley [9] went on to consider $n^3 + 2$. Here he was also able to produce sums of the form $S_I(q; c)$, but now the intervals I were typically of length $q^{1/3}$. Thus he was unable to produce a satisfactory bound using (1) in conjunction with the Weil estimate (4). Instead he made the conjecture that

$$S_{(a,b]}(q; c) \ll q^{\varepsilon}(b-a)^{1/2}, \quad (b - a \leq q,\ q \nmid c),$$

for any fixed $\varepsilon > 0$, and showed, subject to this conjecture, that there is a positive constant δ such that $P(n^3 + 2)/n^{1+\delta}$ is unbounded. In fact his analysis shows that $\delta = 1/31$ is admissable.

This exemplifies a major problem in a great many applications of Kloosterman sums: Can one give a nontrivial bound for $S_I(q; c)$ when I has length less than $q^{1/2}$?

It is possible to do this when q is 'smooth', that is to say, q consists only of small prime factors. The moduli q occuring in Hooley's analysis of $n^3 + 2$ are not necessarily smooth, but Heath-Brown [7] has recently managed to circumvent this difficulty, and to show unconditionally that $P(n^3 + 2)/n^{1+\delta}$ is unbounded, with a positive constant δ. The method produces an explicit value for the constant δ, but the reader might be forgiven for doubting whether δ is indeed positive, for the value obtained is $\delta = 10^{-303}$ (!).

References

1 L.M. Adleman and D.R. Heath-Brown, *The first case of Fermat's last theorem*, Invent. Math., 79 (1985), 409–416.

2 J. Brüdern and E. Fouvry, *Lagrange's four squares theorem with almost prime variables*, J. Reine Angew. Math., 454 (1994), 59–96.

3 J.-M. Deshouillers and H. Iwaniec, *On the greatest prime factor of $n^2 + 1$*, Ann. Inst. Fourier (Grenoble), 32 (1982), 1–11 (1983).

4 E. Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*, Invent. Math., 79 (1985), 383–407.

5 D.R. Heath-Brown, *The fourth power moment of the Riemann zeta-function*, Proc. London Math. Soc. (3), 38 (1979), 385–422.

6 D.R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2), 37 (1986), 27–38.

7 D.R. Heath-Brown, *The largest prime factor of $X^3 + 2$*, to appear.

8 C. Hooley, *On the greatest prime factor of a quadratic polynomial*, Acta Math., 117 (1967), 281–299.

9 C. Hooley, *On the greatest prime factor of a cubic polynomial*, J. reine angew. Math., 303/304 (1978), 21–50.

10 H.D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Mathematica, 49 (1926), 407–464.

11 N.V. Kuznetsov, *The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums*. Mat. Sb. (N.S.), 111(153) (1980), 334–383, 479.

12 Y. Motohashi, *The binary additive divisor problem*, Ann. Sci. École Norm. Sup., (4) 27 (1994), 529–572.

13 A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A., 34, (1948). 204–207.

14 N.I. Zavorotnyi, *On the fourth moment of the Riemann zeta function*, Automorphic functions and number theory, 69–124a, 254, (Akad. Nauk SSSR, Otdel., Vladivostok, 1989).