Western Number Theory Problems, 18 & 21 Dec 1997

Edited by Gerry Myerson

for mailing prior to 1998 (Tiburon) meeting

Summary of earlier meetings & problem sets with old (pre 1984) & new numbering.

1967 Berkeley	1968 Berkeley		1969 Asilomar	
1970 Tucson	1971 Asilomar		1972 Claremont	72:01–72:05
1973 Los Angeles	73:01–73:16		1974 Los Angeles	74:01–74:08
1975 Asilomar	75:01–75:23			
1976 San Diego	1–65	i.e., 76:01–76:65		
1977 Los Angeles	101–148	i.e., 77:01–77:48		
1978 Santa Barbara	151–187	i.e., 78:01–78:37		
1979 Asilomar	201–231	i.e., 79:01–79:31		
1980 Tucson	251–268	i.e., 80:01–80:18		
1981 Santa Barbara	301–328	i.e., 81:01–81:28		
1982 San Diego	351–375	i.e., 82:01–82:25		
1983 Asilomar	401–418	i.e., 83:01–83:18		
1984 Asilomar	84:01–84:27		1985 Asilomar	85:01–85:23
1986 Tucson	86:01–86:31		1987 Asilomar	87:01–87:15
1988 Las Vegas	88:01–88:22		1989 Asilomar	89:01–89:32
1990 Asilomar	90:01–90:19		1991 Asilomar	91:01–91:25
1992 Corvallis	92:01–92:19		1993 Asilomar	93:01–93:32
1994 San Diego	94:01–94:27		1995 Asilomar	95:01–95:19
1996 Las Vegas	96:01–96:18		1997 Asilomar (present set)	97:01–97:22

[With comments on 91:24, 93:13, 95:01, and 95:18]

COMMENTS ON ANY PROBLEM WELCOME AT ANY TIME

Centre for Number Theory Research,
MPCE Building E7A,
Macquarie University,
NSW 2109 Australia
gerrympce.mq.edu.au
Australia-2-9850-8952 fax 9850-8114

24 July 98

Comments on Earlier Problems

91:24 (Dick Katz) Katz asked about $\prod_3^\infty \cos(\pi/k)$. Don Redmond has pointed out that it is discussed in

C. J. Bouwkamp, An infinite product, *Indag. Math.* 27 (1965) 40–46, MR30 #5468

93:13 (Reese Scott) Scott noted that

$$\{\,(x,y,z) : x^2+y^2=z^2, \gcd(x,y,z)=1,\ \#\text{ of prime factors of } xyz \text{ is at most } 5\,\}$$

is a finite set and asked whether 5 could be replaced by 6 or 7.

Kevin Ford used sieves to prove that 5 can't be replaced by 19 (and gave a heuristic argument for replacing 5 by 6).

Remark: Diamond and Halberstam have replaced 19 by 17, using sieves. See

H. Diamond, H. Halberstam, Some applications of sieves of dimension exceeding 1, in G. R. H. Greaves et al., eds., Sieve Methods, Exponential Sums, and their Applications in Number Theory, Cambridge U. Press, 1997.

95:01 (Joel Brenner and Richard Guy) (a question about primes dividing numbers of the form $a^k + b^k$)

Remark: see

Pieter Moree, On the divisors of a^k+b^k, *Acta Arithmetica* 80 (1997) 197-212.

95:18 (Martin LaBar, via Richard Guy) Is there a 3×3 magic square with distinct square entries?

Remark: Lee Sallows discusses (among other things) the problem above and reports that the closest approach to date is a magic square due to Michael Schweitzer containing six squares (marked with an asterisk);

$$\begin{pmatrix} 37629182553169* & 61629448152529 & 102451381817929* \\ 132058870105969* & 67236670841209* & 2414471576449* \\ 32021959864489 & 72843893529889 & 96844159129249* \end{pmatrix}$$

The reference is,

Lee Sallows, The Lost Theorem, *Math. Intell.* 19 (1997) 51–54.

In email of 29 Nov 97, Sallows writes that Schweitzer has many more examples, with smaller entries. Sallows also confirms that the square attributed to Schweitzer in the 1995 problem set (with all entries squares but one diagonal failing) was in fact his (Sallows').

Problems Proposed 18 & 21 Dec 97

97:01 (Josh Benaloh, via Peter Montgomery) Find a family of finite groups and representations such that group composition and equality testing are easy but inversion becomes computationally infeasible as the size grows.

If the group orders are known, one can invert via exponentiation.

Non-examples:

1. Multiplication modulo n, with the conventional representation of $(\mathbf{Z}/n\mathbf{Z})^\times$. Inversion is harder than multiplication but still feasible.

2. Diffie-Hellman. Let p and q be large primes, $q \equiv 1 \pmod{p}$. Let H be the group of pth roots of 1 modulo q. Fix $h \neq 1$ in H. Then h is a generator for H. Let $G = H/\{1\}$. Define a group operation on G by $(h^x, h^y) \to h^{xy}$, where $\gcd(x,p) = \gcd(y,p) = 1$. G is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^\times$, but both composition and inversion are believed to be computationally infeasible for large p.

97:02 (Jeff Lagarias) A problem of Shub and Smale.

Let $f_w(m)$ be the minimum number of steps needed to generate m using 1, addition, and multiplication; let $f_s(m)$ be the minimum number of steps needed to generate m using 1, -1, addition, and multiplication.

Conjecture A. $f_s(n!) \gg_k (\log n)^k$ for each $k \geq 1$.

Conjecture B. $f_w(n!) \gg_k (\log n)^k$ for each $k \geq 1$.

Conjecture A implies P $\neq$ NP in the Blum-Shub-Smale real number model of computation.

M. Shub, S. Smale, On the intractability of Hilbert's Nullstellensatz and an algebraic version of "NP $\neq$ P", *Duke Math. J.* 81 (1996) 47–54, MR 97h:03067

97:03 (Peter Borwein) Let $\mathcal{L}_n = \{ \sum_{j=0}^{n-1} \delta_j x^j : \delta_j = \pm 1 \}$.

1. Let n be prime. Show that every p in $\mathcal{L}_n$ is irreducible if and only if 2 is a primitive root of n.

2. Show that $\max_{p \text{ in } \mathcal{L}_n} \|p\|_3 = \|1 + z + \ldots + z^{n-1}\|_3$, where $\|p\|_3^3 = \frac{1}{2\pi} \int_0^{2\pi} |p(\theta)|^3 \, d\theta$.

97:04 (Michael Filaseta) Let f and g be in $\mathbf{Z}[x]$ with degree around 10^{20} but only 50 to 100 non-zero coefficients. Find a practical algorithm for determining whether $\gcd(f,g) = 1$.

If it helps, assume that each non-zero coefficient of f is 1, and that $g(x) = x^{\deg f} f(x^{-1})$.

97:05 (John Wolfskill) Jeff Lagarias asked (**95:03**) whether, given a number field K, there exists an extension L such that $\mathcal{O}_L$ has a power basis.

For α in $\mathcal{O}_L$, $|D(\alpha)| = D_L m_\alpha^2$, where $m_\alpha = \big[\mathcal{O}_L : \mathbf{Z}[\alpha]\big]$. A common inessential discriminant divisor, or *cidd*, is a prime which divides m_α for all α. Clearly, if there is a cidd, then $\mathcal{O}_L$ has no power basis; it is known that the converse is false.

Is it true that for every $n \geq 3$ there exists an integer m such that if $[K : \mathbf{Q}] = n$ then $L = K(e^{2\pi i/m})$ has no cidd?

It is known that $m = 19$ works for all $n \le 10$, and $m = 159$ works for all $n \le 30$.

97:06 (David Boyd) Conjecture: There are only finitely many n for which there exists a Pisot number β_n such that $\mathbf{Z}[\beta_n] = \mathbf{Z}[2\cos\frac{2\pi}{n}]$.

Recall that a Pisot number is an algebraic integer $\beta > 1$ all of whose other conjugates γ satisfy $|\gamma| < 1$.

The problem arises from a construction of quasicrystals in

J.-P. Gazeau, Pisot-cyclotomic integers for quasilattices, in R. V. Moody, ed., The Mathematics of Long-Range Aperiodic Order, Nato ASI Series C, Vol. 489, Kluwer, 1997, 175–198.

Such a Pisot number exists for $n = 5, 7, 8, 9, 11, 12$, and 15. Computations suggest (but do not prove) there is no such number for $n = 16$. The conjecture is based on an analogue of Bremner's conjecture on power bases for $\mathbf{Z}[e^{2\pi i/p}]$.

97:07 (Neville Robbins) Landau proved $\#\{\, n \le x : n = a^2 + b^2 \,\} \sim b_2 \frac{x}{\sqrt{\log x}}$, where $b_2 = \big(\frac{1}{2}\prod_{q\equiv 3 \pmod 4} \frac{q^2}{q^2-1}\big)^{1/2}$, the product taken over primes only.

Is it true that if p is an odd prime then $\#\{\, n \le x : n = a^2 + pb^2 \,\} \sim b_p \frac{x}{\sqrt{\log x}}$, $b_p = \big(\frac{1}{p}\prod_{(\frac{q}{p})=-1} \frac{q^2}{q^2-1}\big)^{1/2}$?

Solution: Gang Yu of the University of Georgia proves in a preprint that $\#\{\, n \le x : n = a^2 + pb^2 \,\} \sim b_p \frac{x}{\sqrt{\log x}}$ with

$$b_p^2 = f_p \frac{h(\Delta)}{\sqrt{p}} \big(1 - \frac{1}{p}\big)^{-1} \prod_{(\frac{-4q}{p})=-1} \big(1 - q^{-2}\big)^{-1}$$

where $h(\Delta)$ is the class number of $\mathbf{Q}(\sqrt{-p})$ and f_p depends only on the residue class of p (mod 8) (for $p > 3$). From Siegel's estimate on $h(\Delta)$, Yu derives $b_p \gg p^{-\epsilon}$, contradicting the conjecture, which yields $b_p \asymp p^{-1/2}$.

97:08 (Michael Bennett) Are there any solutions to $\frac{x^2-1}{y^2-1} = (z^2-1)^2$, $x, y, z > 1$, other than $(x, y, z) = \big(m(4m^2-3), m, 2m\big)$, $m \ge 2$, and

$$(x, y, z) = (8m^4 + 16m^3 + 8m^2 - 1, 2m^2 + 2m, 2m + 1), \qquad m \ge 1?$$

97:09 (Seva Lev) Let p be an odd prime, let A and B be non-empty sets of residues modulo p. The Cauchy-Davenport Theorem asserts that

$$\#\{\, a + b \,\} \ge \min\{\, p, \#(A) + \#(B) - 1 \,\}.$$

Here, and below, a runs over all elements of A, and b, all elements of B.

The Erdős-Heilbronn Conjecture, recently proved, is

$$\#\{\, a + b : a \ne b \,\} \ge \min\{\, p, \#(A) + \#(B) - 3 \,\}.$$

Are there general estimates for $\#\{\, a+b : (a,b) \notin R \,\}$, where $R \subseteq A \times B$ is any reasonable binary relation? Conjecture:

$$\#\{\, a+b : (a,b) \notin R \,\} \geq \min\{\, p, \#(A) + \#(B) - 3 \,\}$$

for any $R \subseteq A \times B$ satisfying

1. If $(a_1, b) \in R$ and $(a_2, b) \in R$ then $a_1 = a_2$,
2. If $(a, b_1) \in R$ and $(a, b_2) \in R$ then $b_1 = b_2$, and
3. If $(a_1, b_1) \in R$ and $(a_2, b_2) \in R$ then $a_1 + b_1 \neq a_2 + b_2$ unless $(a_1, b_1) = (a_2, b_2)$.

This generalizes Erdős-Heilbronn.

97:10 (Bob Silverman) The question concerns representations $N = \sum_{j=1}^{L} p_j^{\alpha_j}$ where p_j is the jth prime and $\alpha_j \geq 1$, e.g., $23 = 2 + 3^2 + 5 + 7$.

1. Is 33 the largest N not so representable?
2. How many different representations are there as $N \to \infty$?
3. How do α_j and L behave as $N \to \infty$?

97:11 (Bob Silverman) Let $N = pq$, p, q odd primes. Then

$$\#\{\, r \text{ in } \mathbf{Z}/N\mathbf{Z} : \text{ order of } r \text{ is } \lambda(N) \,\} > \frac{2e^{-\gamma}}{3} \frac{N}{\log\log N}.$$

1. Can $\frac{2e^{-\gamma}}{3}$ be improved?
2. Suppose $0 < \delta < 1/16$ and $N^{\delta} \geq 2$. Then

$$\#\{\, r \text{ in } \mathbf{Z}/N\mathbf{Z} : (\text{order of } r) \geq N^{-\delta}\lambda(N) \,\} > e^{-\gamma} \frac{N}{\log\log N}.$$

Is this best possible? Note: $\lambda(N) = \text{ lcm}\{\, p-1, q-1 \,\}$.

97:12 (Bob Silverman) Let $N = pq$, p, q odd primes. Assuming the truth of the following propositions, find a zero-knowledge proof.

1. $\gcd(p-1, q-1) < N^{\epsilon}$ for any $\epsilon > 0$,
2. $p-1$ does not divide $q-1$,
3. $p-1$ and $q-1$ each have at most $[\log\log N]$ distinct prime factors.

Remark: Peter Montgomery solves (2); The prover exhibits a base b such that $\gcd(b^N - b, N) = 1$. If $p-1 \mid q-1$ then $p-1 \mid (q-1) + (p-1)q = N-1$, hence $p \mid b^N - b$ and $p \mid N$, contradiction; hence, $p-1$ does not divide $q-1$.

$N = pq$ is not a Carmichael number so there are many b such that N does not divide $b^N - b$. Try $b = 2, 3, 5, \ldots$. If the first b such that N does not divide $b^N - b$ has a common factor with N, then p and q are easy to find.

97:13 (John Brillhart) Let $P_2(x)$ be the number of base 2 pseudoprimes not exceeding x. Decide the following conjectures.

(1a) $P_2(10^n)/P_2(10^{n-1})$, $n = 4, 5, \ldots$, is a decreasing sequence.

(1b) $\rho = \lim_{n\to\infty} P_2(10^n)/P_2(10^{n-1})$ exists, and $1 < \rho < 3$.

(2a) $\pi(10^n)/\pi(10^{n-1})$, $n = 2, 3, \ldots$, is an increasing sequence (Lowell Schoenfeld proved this for n sufficiently large).

(2b) $\Delta\pi(10^n)/\Delta\pi(10^{n-1})$, $n = 3, 4, \ldots$, is an increasing sequence. Here, $\Delta f(n)$ means $f(n) - f(n-1)$.

(3) $\Delta P_2(10^n)/\big(\Delta\pi(10^n) + \Delta P_2(10^n)\big) < 3^{-n}$ for $n \geq 10$.

These heuristic conjectures are based on counts up to 10^{13}.

Remark: Carl Pomerance points out that

P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* 4 (1956) 201–206

conjectures $P_2(x) > x^{1-\epsilon}$ for every $\epsilon > 0$ and every $x > x(\epsilon)$. In fact, Erdős conjectures this lower bound not just for $P_2(x)$ but for $C(x)$, the number of Carmichael numbers not exceeding x. If the limit in (1b) exists (and the Erdős heuristic supports the existence of this limit), then the Erdős conjecture implies that the limit is 10. If the Erdős conjecture is true, then (3) is also false, even if the 3 in the problem is replaced by $1 + \epsilon$. In

D. Shanks, Solved and Unsolved Problems in Number Theory, Chelsea, 1985

Conjecture 21 is that $P_2(N)/N^{1/2-\epsilon}$ increases without bound for any positive ϵ. If true, this suggests that the limit in (1b), if it exists, is at least $\sqrt{10} > 3$. Shanks considers the possibility that $\sqrt{N}/(\log N)^2 < P_2(N) < \sqrt{N}/\sqrt{\log N}$, but decides that there is insufficient evidence to warrant a conjecture.

Pomerance further notes that the Rosser-Schoenfeld error estimates for the prime number theorem enable one to work out an n_0 beyond which the inequalities in (2a) and (2b) hold; if n_0 is small enough, one can check the remaining cases by computer.

97:14 (Bart Goddard) The formula $f(n) = \sum_{k=0}^{\lceil \frac{n}{2}-1 \rceil} \binom{n-k-1}{k}$ for Fibonacci numbers was extended to rational arguments by Halsey, using beta functions:
$B(m,n) = \int_0^1 x^{n-1}(1-x)^{m-1}\,dx$; $\binom{n}{m} = \frac{1}{(n+1)B(m+1,n-m+1)}$ for m, n in $\mathbf{R}$;

$$f(u) = \sum_{k=0}^{\lceil \frac{u}{2}-1 \rceil} \big((u-k)\int_0^1 x^{u-2k-1}(1-x)^k\,dx\big)^{-1}.$$

However, $f(u) = f(u-1) + f(u-2)$ fails for non-integer u. Tweak Halsey's formula to restore the identity for all rational u.

Halsey, The Fibonacci number F_u where u is not an integer, *Fib. Q.* 3 (1965) 147–152

97:15 (Peter Montgomery) Given a positive integer n, let $f(n)$ be the number of ways for two people to exchange n dollars, using the minimum number of bills of standard U.S. denominations (1, 5, 10, 20, 50, 100). For example, $f(13) = 3$ because there are three ways to make \$13 with 4 bills ($10 + 1 + 1 + 1$, $10 + 5 - 1 - 1$, and $20 - 5 - 1 - 1$), and no way using fewer bills.

What is the range of f? What ranges are possible, using other currency systems?

97:16 (Gerry Myerson) Do there exist integers, $a_1, \ldots, a_n$, not necessarily distinct, such that each of the $n+1$ integers $1, 2, 4, \ldots, 2^n$ can be obtained as $\sum_{j\in J} a_j$ for some subset J of $\{1, \ldots, n\}$? The answer is no for $n \le 3$.

Solution: Peter Montgomery shows that the answer is yes for $n \ge 4$. For $n = 4$, let $a_1, \ldots, a_4$ be $-5, 1, 7, 9$; then $1 = 1$, $2 = -5 + 7$, $4 = -5 + 9$, $8 = 1 + 7$, and $16 = 7 + 9$. For $n > 4$, let $a_1, \ldots, a_4$ be as above, and let $a_j = 2^j$ for $5 \le j \le n$.

Remark: David Moulton notes that the numbers $-5(32)^j, 32^j, 7(32)^j, 9(32)^j$, $0 \le j \le k-1$, are $4k$ integers from which the $5k$ numbers $1, 2, 4, \ldots, 2^{5k-1}$ can be obtained as subset sums. So perhaps the real problem is to find $f(n)$, the smallest number of integers required to express $1, 2, 4, \ldots, 2^n$ as subsums. From the above, $f(n) = n+1$ for $0 \le n \le 3$, $f(n) \le n$ for $n \ge 4$, and $f(n) < (.8 + \epsilon)n$ for $n > n_0(\epsilon)$.

The editor notes that $1, -5(16)^j, 7(16)^j, 9(16)^j$, $0 \le j \le k-1$, are $3k+1$ integers from which the $4k+1$ numbers $1, 2, 4, \ldots, 2^{4k}$ can be obtained as subset sums;

$$2^{4j+1} = -5(16)^j + 7(16)^j, \qquad 2^{4j+2} = -5(16)^j + 9(16)^j,$$
$$2^{4j+3} = 7(16)^{j-1} + 9(16)^{j-1} + 7(16)^j, \qquad 2^{4j+4} = 7(16)^j + 9(16)^j.$$

Thus, $f(n) < (.75 + \epsilon)n$ for $n > n_0(\epsilon)$. See also 97:19.

In email of 29 Jan 98, David Moulton reports that from the five numbers -20, -15, 17, 19, 28 the first 7 powers of 2 can be obtained as subset sums. Then $5k$ numbers suffice to obtain $7k$ powers, and $f(n) < (\frac{5}{7} + \epsilon)n$ for $n > n_0(\epsilon)$. He has further small improvements.

97:17 (Hugh Edgar) 1. Are there infinitely many totally real non-normal cubic extensions K of $\mathbf{Q}$ for which $\mathcal{O}_K$ has a power basis?

2. Are there infinitely many cyclic quartic extensions K of $\mathbf{Q}$ for which $\mathcal{O}_K$ has a power basis?

Remark: John Wolfskill writes, in regard to the first question, for a prime $p \ge 11$, consider the cubic $f(x) = x^3 - px + p$. This has discriminant $p^2(4p - 27)$ and three real roots. Let $\mathbf{K} = \mathbf{Q}(\alpha)$, where α is a root of f. Now f is Eisenstein with respect to p, which implies that p is totally ramified in $\mathbf{K}$ and so p^2 divides the discriminant of $\mathbf{K}$. If $4p - 27$ is squarefree, then $\mathbf{K}$ is a totally real non-normal cubic extension of $\mathbf{Q}$ with integral basis 1, α, α^2.

Adolf Hildebrand argues that $S(x) = \#\{p < x : ap + b \text{ is squarefree}\}$ is asymptotic (excluding degenerate cases) to $Cx/\log x$ for some positive constant C depending on a and b (so, in particular, there are infinitely many primes such that $4p - 27$ is squarefree, and infinitely many totally real non-normal cubic extensions K of $\mathbf{Q}$ for which $\mathcal{O}_K$ has a power basis):

Writing the characteristic function of the squarefree numbers, $\mu^2(n)$, as $\sum_{d^2|n} \mu(d)$ leads to

$$S(x) = \sum_{d<\sqrt{x}} \mu(d) S(x, d),$$

where $S(x,d) = \#\{\, p : ap+b < x, d^2 \mid ap+b \,\}$. Now, $S(x,d)$ is, up to an error $O(1)$, the number of primes $p < x/a$ that lie in a certain arithmetic progression modulo d^2. For any fixed d, this can be estimated by Dirichlet or Siegel-Walfisz; for general d, by Brun-Titchmarsh. Altogether, it follows that $S(x)$ is asymptotic to a constant multiple of $\pi(x)$.

97:18 (John Friedlander) Given a prime $p \equiv 1 \pmod 4$, define the spin of p, $\sigma(p)$, to be the Jacobi symbol $\left(\frac{a}{b}\right)$, where a, b are the unique positive integers such that $p = a^2 + b^2$ and b is odd. Give an elementary proof that

1. $\sigma(p) = 1$ for infinitely many p, and
2. $\sigma(p) = -1$ for infinitely many p.

Remark: Friedlander and Iwaniec have a long, complicated proof of the stronger result, $\sum_{p \le x} \sigma(p) \ll x^{1-\delta}$ for some $\delta > 0$.

97:19 (Seva Lev) Given $n+1$ distinct integers $b_1, \ldots, b_{n+1}$, find reasonable conditions for the existence of an n-element set of integers (or rationals) A such that all the b_j are contained in the set of all subset sums of A. E.g., $\{\, 1, c, c^2, \ldots, c^n \,\}$ can't be obtained this way for $c > c_0(n)$ ($c = n^{n/2} + 1$ will do), as the elements grow too fast.

97:20 (Ernie Croot, III) For $n = p_1^{a_1} \times \ldots \times p_k^{a_k}$, let $\Omega(n) = a_1 + \ldots + a_k$. Suppose $\epsilon > 0$, p prime, and $0 \le h \le p-1$.

1. Find a good upper bound on $B(p,\epsilon,h) = \Omega\big(\prod_{0 \le n \le \log^{1+\epsilon} p}(np+h)\big)$.
2. Is it true that $B(p,\epsilon,h) = \log^{1+\epsilon+o(1)} p$ as $p \to \infty$?

97:21 (Shuguang Li) Let $N_a(x)$ be the number of positive integers $n \le x$ such that $\gcd(a,n) = 1$ and a has maximal order (mod n). It has been proved that

(i) $\limsup_{x\to\infty} x^{-2} \sum_{1 \le a \le x} N_a(x) > 0$,

(ii) $\liminf_{x\to\infty} x^{-2} \sum_{1 \le a \le x} N_a(x) = 0$, and

(iii) for all a, $\liminf_{x\to\infty} x^{-1} N_a(x) = 0$.

Does there exist a such that $\limsup_{x\to\infty} x^{-1} N_a(x) > 0$? If so, find all such a.

Li conjectures that $\limsup_{x\to\infty} x^{-1} N_a(x) > 0$ for all a not in $\mathcal{E}$, where

$$\mathcal{E} = \{\, a : |a| \le 1, \text{ or } |a| \text{ is twice a square, or } |a| = b^q \text{ for some } b \text{ and some prime } q \,\}.$$

97:22 (John Selfridge) Let $n = rs^2$, r square-free, $r > 1$. It is conjectured that for all such n except $n = 8$ and $n = 392$ there exist integers a, b with $n < a < b < r(s+1)^2$ such that nab is a square.