NUMBER THEORY

Any common factor of two of such numbers would have to be divisible by 2, 3, 5 or 7. So it is sufficient to prove that among any ten consecutive integers there is at least one that is not divisible by 2, 3, 5 or 7. We get such an integer by elimination as follows. Strike out those divisible by 3. There may be either 3 or 4 of them. Among these there is either at least one or two respectively that are divisible also by 2. Thus if we strike off also those that are divisible by 2 we will have eliminated at most seven of the integers. Note that by so doing we have stricken off at least one number divisible by five. Thus we are left with three integers only two of which can be divisible by 5 or 7.

B1. (176, 25, 0, 0, 0, 0, 0, 0, 1, 1, 1, 4)

A composite (positive integer) is a product \( ab \) with \( a \) and \( b \) not necessarily distinct integers in \( \{2, 3, 4, \ldots\} \). Show that every composite is expressible as \( xy + xz + yz + 1 \), with \( x \), \( y \), and \( z \) positive integers.

Solution. Substituting \( z = 1 \) yields \((y + 1)(y + 1)\), so to represent the composite number \( n = ab \) with \( a, b \geq 2 \), let \((x, y, z) = (a - 1, b - 1, 1)\).

Remark. Although the problem asks only about representing composite numbers, all but finitely many prime numbers are representable too. Theorem 1.1 of [BC] proves that the only positive integers not of the form \( xy + xz + yz + 1 \) for integers \( x, y, z > 0 \) are the 19 integers 1, 2, 3, 5, 7, 11, 19, 23, 31, 43, 59, 71, 79, 103, 131, 191, 211, 331, and 463, and possibly a 20th integer greater than \( 10^{11} \). Moreover, if the Generalized Riemann Hypothesis (GRH) is true, then the 20th integer does not exist. (See [Le] for earlier work on this problem.)

The situation is analogous to that of the class number 1 problem: for many years it was known that the squarefree integers \( d > 0 \) such that \( \mathbb{Q}(\sqrt{-d}) \) has class number 1 were

\[
d = 1, 2, 3, 7, 11, 19, 43, 67, 163
\]

and possibly one more; the existence of this tenth imaginary quadratic field of class number 1 was eventually ruled out: see the appendix to [Se3] for the history and the connection of this problem to integer points on modular curves.

In fact, researchers in the 19th century connected the problem of determining the positive integers representable by \( xy + xz + yz + 1 \) to problems about class numbers of quadratic imaginary fields, or equivalently class numbers of binary quadratic forms: [Mord1] mentions that the connection is present in comments by Liouville, in Journ. de maths., series 2, tome 7, 1862, page 44, on a paper by Hermite. See also [Bel], [Wh], and [Mord2, p. 291]. The GRH implies the nonexistence of a Siegel zero for the Dirichlet \( L \)-functions associated to these fields, and this is what is used in the proof of Theorem 1.1 of [BC].


95

A1. (92, 2, 6, 7, 0, 0, 0, 9, 2, 8, 32)

How many primes among the positive integers, written as usual in base 10, are such that their digits are alternating 1's and 0's, beginning and ending with 1?

Answer. There is only one such prime: 101.

Solution. Suppose that \( N = 101 \ldots 0101 \) with \( k \) ones, for some \( k \geq 2 \). Then

\[
99N = 9999 \ldots 9999 = 10^{2k} - 1 = (10^k + 1)(10^k - 1).
\]

If moreover \( N \) is prime, then \( N \) divides either \( 10^k + 1 \) or \( 10^k - 1 \), and hence one of \( \frac{10^k+1}{N} \) and \( \frac{10^k-1}{N} \) is an integer. For \( k > 2 \), \( 10^k - 1 \) and \( 10^k + 1 \) are both greater than 99, so we get a contradiction. Therefore \( k = 2 \) and \( N = 101 \) (which is prime).
B1. (83, 29, 9, 0, 0, 0, 0, 0, 6, 10, 38, 32)

Find the smallest positive integer n such that for every integer m, with
0 < m < 1993, there exists an integer k for which
\[ \frac{m}{1993} < \frac{k}{n} < \frac{m+1}{1994}. \]

Answer. The smallest positive integer n satisfying the condition is n = 3987.

Lemma 1. Suppose a, b, c, and d are positive numbers, and \( \frac{a}{b} < \frac{c}{d} \). Then
\[ \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}. \]

This lemma is sometimes called the mediant property or the règle des nombres moyens [Nel, pp. 60–61]. It appears without proof in the Triparty en la Science des Nombres, which was written by the French physician Nicholas Chuquet in 1484 (although his work went unpublished until 1880). It is not hard to verify this inequality directly, but there is an even easier way of remembering it: If a sports team wins a of b games in the first half of a season, and c of d games in the second half, then its overall record \((a+c)/(b+d)\) is between its records in its two halves \((a/b \text{ and } c/d)\). Alternatively, Figure 24 gives a “proof without words.” For three more proofs without words of this result, see [Nel, pp. 60–61].

![Figure 24.](image)

A proof without words of Lemma 1.

Solution 1. By Lemma 1,
\[ \frac{m}{1993} < \frac{2m+1}{3987} < \frac{m+1}{1994}. \]

We will show that 3987 is best possible. If
\[ \frac{1992}{1993} < \frac{k}{n} < \frac{1993}{1994} \]
then
\[ \frac{1}{1993} > \frac{n-k}{n} > \frac{1}{1994}, \]
so
\[ 1993 < \frac{n}{n-k} < 1994. \]

Clearly \( n-k \neq 1 \), so \( n-k \geq 2 \). Thus \( n > 1993(n-k) \geq 3986 \), and \( n \geq 3987 \).

Solution 2. Subtracting everything in the desired inequality from 1, and using the change of variables \( M = 1993 - m, K = n - k \), the problem becomes: determine the smallest positive integer n such that for every integer M with \( 1993 > M > 0 \), there exists an integer K for which
\[ \frac{M}{1993} < \frac{K}{n} < \frac{M}{1994}, \]
or equivalently, \( 1993K < nM < 1994K \).

For \( M = 1 \), K cannot be 1 and hence is at least 2, so \( n > 1993 \cdot 2 = 3986 \). Thus \( n \geq 3987 \). On the other hand n = 3987 works, since then for each M, K = 2M satisfies the inequalities.
Solution 3 (Naoki Sato).

Lemma 2. Let $a$, $b$, $c$, $d$, $p$, and $q$ be positive integers such that $a/b < p/q < c/d$, and $bc - ad = 1$. Then $p \geq a + c$ and $q \geq b + d$.

Proof. Since $bp - aq > 0$, $bp - aq \geq 1$. Also, $cq - dp > 0$, so $cq - dp \geq 1$. Hence $d(bp - aq) + b(cq - dp) \geq b + d$, which simplifies to $(bc - ad)q \geq b + d$. But $bc - ad = 1$, so $q \geq b + d$. The proof of $p \geq a + c$ is similar.

Now \[ \frac{1992}{1993} < \frac{k}{n} \leq \frac{1993}{1994} \] for some $k$, and $1993 \cdot 1994 - 1992 \cdot 1994 = 1$, so $n \geq 1993 + 1994 = 3987$. And $n = 3987$ works, by Lemma 1.

Remark. Looking at (1) was key. What clues suggest that it would be helpful to look at large $m$?

Remark. This problem and Lemma 2 especially are related to the beautiful topic of Farey series: see [Hon1, Essay 5].

A3. (95, 44, 39, 0, 0, 0, 0, 12, 5, 3, 6)

The number $d_1d_2 \ldots d_9$ has nine (not necessarily distinct) decimal digits. The number $e_1e_2 \ldots e_9$ is such that each of the nine 9-digit numbers formed by replacing just one of the digits $d_i$ in $d_1d_2 \ldots d_9$ by the corresponding digit $e_i$ ($1 \leq i \leq 9$) is divisible by 7. The number $f_1f_2 \ldots f_9$ is related to $e_1e_2 \ldots e_9$ in the same way: that is, each of the nine numbers formed by replacing one of the $e_i$ by the corresponding $f_i$ is divisible by 7. Show that, for each $i$, $d_i - f_i$ is divisible by 7. [For example, if $d_1d_2 \ldots d_9 = 199501996$, then $e_6$ may be 2 or 9, since 199502996 and 199500996 are multiples of 7.]

Solution. Let $D$ and $E$ be the numbers $d_1 \ldots d_9$ and $e_1 \ldots e_9$, respectively. We are given that

\[
(e_i - d_i)10^{9-i} + D \equiv 0 \pmod{7}
\]
\[
(f_i - e_i)10^{9-i} + E \equiv 0 \pmod{7}
\]

for $i = 1, \ldots, 9$. Sum the first relation over $i = 1, \ldots, 9$ to get $E - D + 9D \equiv 0 \pmod{7}$, or equivalently $E + D \equiv 0 \pmod{7}$. Now add the first and second relations for any particular value of $i$ to get $(f_i - d_i)10^{9-i} + E + D \equiv 0 \pmod{7}$. Since $E + D$ is divisible by 7, and 10 is coprime to 7, we conclude $d_i - f_i \equiv 0 \pmod{7}$.

2000 B2. (114, 7, 2, 0, 0, 0, 0, 0, 2, 6, 35, 29)

Prove that the expression

\[
\frac{\gcd(m, n)}{n} \binom{n}{m}
\]

is an integer for all pairs of integers $n \geq m \geq 1$.

Solution 1. Let $a = \frac{m}{\gcd(m, n)}$ and $b = \frac{n}{\gcd(m, n)}$. Then

\[
\frac{a}{b} \binom{n}{m} = \frac{m}{n} \binom{n}{m} = \frac{n}{m-1}
\]

is an integer, so $b \mid a^n$. But $\gcd(a, b) = 1$, so $b \mid \binom{n}{m}$. Hence

\[
\frac{\gcd(m, n)}{n} \binom{n}{m} = \frac{1}{b} \binom{n}{m}
\]
Solution 2. Since \( \gcd(m, n) \) is an integer linear combination of \( m \) and \( n \), it follows that

\[
\frac{\gcd(m, n)}{n} \left( \frac{n}{m} \right)
\]

is an integer linear combination of the integers

\[
\frac{m}{n} \left( \frac{n}{m} \right) = \left( \frac{n}{m} - 1 \right) \quad \text{and} \quad \frac{n}{m} \left( \frac{n}{m} \right) = \left( \frac{n}{m} \right)
\]

and hence is itself an integer.

Solution 3. To show that a nonzero rational number is an integer, it suffices to check that the exponent of each prime in its factorization is nonnegative. So let \( p \) be a prime, and suppose that the highest powers of \( p \) dividing \( n \) and \( m \) are \( p^a \) and \( p^b \), respectively. If \( a \leq b \), then \( p \) has a nonnegative exponent in both \( \gcd(m, n) / n \) and in \( \left( \frac{n}{m} \right) \). If \( a > b \), it suffices to show that \( \left( \frac{n}{m} \right) \) is divisible by \( p^{a-b} \), but this follows from Kummer's Theorem, described in Solution 2 to 1997A5.

2000 A2. (150, 1, 0, 0, 0, 0, 0, 1, 0, 23, 20)

Prove that there exist infinitely many integers \( n \) such that \( n, n+1, n+2 \) are each the sum of two squares of integers. [Example: \( 0 = 0^2 + 0^2, 1 = 0^2 + 1^2 \), and \( 2 = 1^2 + 1^2 \).]

In all of the following solutions, we take \( n = x^2 - 1 \). Then \( n+1 = x^2 + 0^2 \), \( n+2 = x^2 + 1^2 \) and it suffices to exhibit infinitely many \( x \) so that \( x^2 - 1 \) is the sum of two squares.

Solution 1. Let \( a \) be an even integer such that \( a^2 + 1 \) is not prime. (For example, choose \( a = 10k + 2 \) for some integer \( k \geq 1 \), so that \( a^2 + 1 = 100k^2 + 40k + 5 \) is divisible by \( 5 \).) Then we can write \( a^2 + 1 \) as a difference of squares \( x^2 - b^2 \), by factoring \( a^2 + 1 \)

as \( rs \) with \( r \geq s > 1 \), and setting \( x = (r+s)/2, b = (r-s)/2 \). (These are integers because \( r \) and \( s \) must both be odd.) It follows that \( x^2 - 1 \) is the sum of two squares \( a^2 + b^2 \), as desired.

Solution 2. The equation \( u^2 - 2v^2 = 1 \) is an example of Pell's equation [NZM, Section 7.8], so it has infinitely many solutions, and we can take \( x = u \).

Remark. The positive integer solutions to \( u^2 - 2v^2 = 1 \) are the pairs \( (u, v) \) satisfying \( u + v\sqrt{2} = (1 + \sqrt{2})^n \) for some \( n \geq 1 \). Incidentally, the positive possibilities for \( v \) are the same as the odd terms in the sequence \( (a_n)_{n \geq 0} \) of Problem 1999A3.

Solution 3. Take \( x = 2a^2 + 1 \); then \( x^2 - 1 = (2a)^2 + (2a)^2 \).

Solution 4 (Abhinav Kumar). If \( x^2 - 1 \) is the sum of two squares, then so is \( x^4 - 1 \), using

\[
x^4 - 1 = (x^2 - 1)(x^2 + 1)
\]

and the identity

\[
(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2
\]

(obtained by computing the norm of \((a+bi)(c+di)\) in two ways). Hence by induction on \( n \), if \( x^2 - 1 \) is the sum of two squares (for instance, if \( x = 3 \)) then so is \( (x^2)^n - 1 \) for all nonnegative integers \( n \).

Related question. Let \( S = \{ a^2 + b^2 : a, b \in \mathbb{Z} \} \). Show that \( S \) does not contain four consecutive integers. But show that \( S \) does contain a (nonconstant) 4-term arithmetic progression.
Related question. Does $S$ contain an arithmetic progression of length $k$ for every integer $k \geq 1$? This is currently an unsolved problem! A positive answer would follow from either of the following conjectures:

- Dickson’s Conjecture. Given linear polynomials $a_1 n + b_1, \ldots, a_k n + b_k$ in $n$, with $a_i, b_i \in \mathbb{Z}$ and $a_i > 0$ for all $i$, such that no prime $p$ divides $(a_1 n + b_1) \cdots (a_k n + b_k)$ for all $n \in \mathbb{Z}$, there exist infinitely many integers $n \geq 1$ such that the values $a_1 n + b_1, \ldots, a_k n + b_k$ are simultaneously prime. (The hypothesis that $p$ does not divide $(a_1 n + b_1) \cdots (a_k n + b_k)$ is automatic if $p > k$ and $p \nmid \gcd(a_1, b_1) \cdots \gcd(a_k, b_k)$, so checking it for all $p$ is a finite computation.)

The special case $a_1 = \cdots = a_k = 1$ of Dickson’s Conjecture is the qualitative form of the Hardy-Littlewood Prime $k$-tuple Conjecture, which itself is a generalization of the Twin Prime Conjecture, which is the statement that there exist infinitely many $n \geq 1$ such that $n$ and $n + 2$ are both prime. On the other hand, Dickson’s Conjecture is a special case of “Hypothesis H" of Schinzel and Sierpiński, in which the linear polynomials are replaced by distinct irreducible polynomials $f_1(n), \ldots, f_k(n)$ with positive leading coefficients. Moreover, for each of these conjectures, there is a heuristic that predicts that the number of $n$ less than or equal to $x$ satisfying the conclusion is $(c + o(1)) x / (\ln x)^k$ as $x \to \infty$, where $c$ is a constant given by an explicit formula in terms of the $k$ polynomials. (See 1988A3 for the definition of $o(1)$.) The quantitative form of Hypothesis H is known as the Bateman-Horn Conjecture. For more on all of these conjectures, see Chapter 6 of [Ri], especially pages 372, 391, and 409.

- A conjecture of P. Erdős. If $T$ is a set of positive integers such that $\sum_{n \in T} 1/n$ diverges, then $T$ contains arbitrarily long finite arithmetic progressions. Erdős, who frequently offered cash rewards for the solution to problems, offered his highest-valued reward of $3000 for a proof or disproof of this statement. See [GrI, p. 24] or [Guy, p. 16].

Let us explain why either of the two conjectures above would imply that our set $S$ contains arithmetic progressions of arbitrary length. We will use the theorem mentioned in 1991B5, that any prime congruent to 1 modulo 4 is in $S$.

Fix $k \geq 4$, and let $\ell_i(n) = 4n + 1 + i(k!)$ for $i = 1, 2, \ldots, k$. Let $P(n) = \ell_1(n) \ell_2(n) \cdots \ell_k(n)$. If $p$ is prime and $p \leq k$, then $p$ does not divide $P(0)$. If $p$ is prime and $p > k$, then for each $i$, the set $\{ n \in \mathbb{Z} : p \mid \ell_i(n) \}$ is a residue class modulo $p$, so there remains at least one residue class modulo $p$ consisting of $n$ such that $p \nmid P(n)$. Hence Dickson’s Conjecture predicts that there are infinitely many $n$ such that $\ell_1(n), \ldots, \ell_k(n)$ are simultaneously prime. Each of these $k$ primes would be congruent to 1 modulo 4, and hence would be in $S$.

Now we show that the conjecture of Erdős implies that $S$ contains arithmetic progressions of arbitrary length, and even better, that the subset $T$ of primes congruent to 1 mod 4 contains such progressions. It suffices to prove that $\sum_{p \in T} 1/p$ diverges, or equivalently that $\lim_{s \to 1^+} \sum_{p \in T} 1/p^s = \infty$. The proof of Dirichlet’s Theorem on primes in arithmetic progressions gives a precise form of this, namely:

$$\lim_{s \to 1^+} \left( \sum_{p \in T} \frac{1}{p^s} \right) / \left( \ln \frac{1}{s-1} \right) = \frac{1}{2}.$$  

Since $\lim_{s \to 1^+} \ln \frac{1}{s-1} = \infty$, this implies $\lim_{s \to 1^+} \sum_{p \in T} 1/p^s = \infty$.

More generally, one says that a subset $P$ of the set of prime numbers has Dirichlet density $\alpha$ if

$$\lim_{s \to 1^+} \left( \sum_{p \in P} \frac{1}{p^s} \right) / \left( \ln \frac{1}{s-1} \right) = \alpha.$$  

Dirichlet’s Theorem states that if $a$ and $m$ are relatively prime positive integers, then the Dirichlet density of the set of primes congruent to $a$ modulo $m$ equals $1/\phi(m)$, where $\phi(m)$ is the Euler $\phi$-function defined in 1985A4. See Theorem 2 in Chapter VI, §4 of [Sel] for details.
A4. \((39, 27, 52, 0, 0, 0, 0, 0, 0, 49, 7, 14, 11)\)

Let \(A_1 = 0\) and \(A_2 = 1\). For \(n > 2\), the number \(A_n\) is defined by concatenating the decimal expansions of \(A_{n-1}\) and \(A_{n-2}\) from left to right. For example \(A_3 = A_2A_1 = 10\), \(A_4 = A_3A_2 = 101\), \(A_5 = A_4A_3 = 10110\), and so forth. Determine all \(n\) such that \(11\) divides \(A_n\).

**Answer.** The number \(11\) divides \(A_n\) if and only if \(n \equiv 1 \pmod{6}\).

**Solution.** The number of digits in the decimal expansion of \(A_n\) is the \(n\)th Fibonacci number \(F_n\). It follows that the sequence \(\{A_n\}\) modulo 11 satisfies a recursion:

\[
A_n = 10^{E_{n-2}}A_{n-1} + A_{n-2} \\
\equiv (-1)^{E_{n-2}}A_{n-1} + A_{n-2} \pmod{11}.
\]

By induction, \(F_n\) is even if and only if 3 divides \(n\); hence \((-1)^{E_{n-2}}\) is periodic with period 3.

Computing \(A_n\) modulo 11 for small \(n\) using the recursion, we find

\[
A_1, \ldots, A_8 \equiv 0, 1, -1, 2, 1, 1, 0, 1 \pmod{11}.
\]

By induction, we deduce that \(A_{n+6} \equiv A_n \pmod{11}\) for all \(n\), and so \(A_n\) is divisible by 11 if and only if \(n \equiv 1 \pmod{6}\).

**Remark.** See 1988A5 for more on linear recursions and Fibonacci numbers.