1955  B4. Do there exist 1,000,000 consecutive integers each of which contains a repeated prime factor?

**First Solution.** We shall prove that there are sequences of consecutive integers of arbitrary length each of which has a repeated prime factor. The proof is by induction on the length. Obviously there are such sequences of length 1.

Suppose \(a_1, a_2, \ldots, a_k\) are \(k\) consecutive integers (in order), each of which has a repeated prime factor. Let \(b = a_1a_2 \cdots a_k\). Then for any integer \(n\)

\[
nb + a_1, \quad nb + a_2, \quad \ldots, \quad nb + a_k
\]

are \(k\) consecutive integers, each of which has a repeated prime factor since \(a_i\) divides \(nb + a_1\). Let \(p\) be a prime not dividing \(b\). Then we can choose \(n\) so that \(nb + a_i + 1\) is divisible by \(p^2\), since this amounts to solving the congruence \(bx + a_k + 1 \equiv 0 \pmod{p^2}\) and \(b\) is relatively prime to \(p^2\). Then each of the \(k + 1\) consecutive integers

\[
nb + a_1, \quad nb + a_2, \quad \ldots, \quad nb + a_k, \quad nb + a_k + 1
\]

has a repeated prime factor.

It follows that there are sequences of consecutive integers of arbitrary length, and in particular sequences of length 1,000,000, each of which has a repeated prime factor.

**Second Solution.** Let \(p_1, p_2, \ldots, p_s\) be \(s\) distinct primes. According to the Chinese Remainder Theorem the simultaneous congruences

\[
x \equiv -1 \pmod{p_1^2} \\
x \equiv -2 \pmod{p_2^2} \\
\ldots \\
x \equiv -s \pmod{p_s^2}
\]

have a solution, say \(n\). Then the \(s\) consecutive integers

\[
n + 1, \quad n + 2, \quad \ldots, \quad n + s
\]

each have a repeated prime factor, for \(p_i^2\) divides \(n + i\). Since we may take \(s = 1,000,000\), there do exist sequences of 1,000,000 consecutive integers, each of which contains a repeated prime factor.


1956  A2. Prove that every positive integer has a multiple whose decimal representation involves all ten digits.

**Solution.** If \(n\) is a positive integer and \(p\) is any other positive integer, then one of the integers

\[
p + 1, \quad p + 2, \quad \ldots, \quad p + n
\]

is a multiple of \(n\). Given \(n\), choose \(p = 1,234,567,890 \times 10^k\), where \(k\) is so large that \(10^k > n\). Then all of the integers \(p + 1, p + 2, \ldots, p + n\) have decimal representations beginning with 1234567890 \ldots, and one of these is a multiple of \(n\).
A-3. If \( x \) is an integer then \( x^2 \equiv 0, 1, 4, 6 \) or 9 (mod 10). The case \( x^2 \equiv 0 \) (mod 10) is eliminated by the statement of the problem. If \( x^2 \equiv 11, 55 \) or 99 (mod 100), then \( x^2 \equiv 3 \) (mod 4) which is impossible. Similarly, \( x^2 \equiv 66 \) (mod 100) implies \( x^2 \equiv 2 \) (mod 4) which is also impossible. Therefore \( x^2 \equiv 44 \) (mod 100). If \( x^2 \equiv 4444 \) (mod 10,000), then \( x^2 \equiv 12 \) (mod 16), but a simple check shows that this is impossible. Finally note that \( (38)^2 = 1444 \).

A-5. Assume that \( n \) divides \( 2^n - 1 \) for some \( n > 1 \). Since \( 2^n - 1 \) is odd, \( n \) is odd. Let \( p \) be the smallest prime factor of \( n \). By Euler's Theorem, \( 2^\phi(p) = 1 \) (mod \( p \)), because \( p \) is odd. If \( \lambda \) is the smallest positive integer such that \( 2^\lambda \equiv 1 \) (mod \( p \)) then \( \lambda \) divides \( \phi(p) = p - 1 \). Consequently \( \lambda \) has a smaller prime divisor than \( p \). But \( 2^n \equiv 1 \) (mod \( p \)) and so \( \lambda \) also divides \( n \). This means that \( n \) has a smaller prime divisor than \( p \).

Contradiction.

A-3.

\[
F(n) = 1 + 2n + 3n^2 + \cdots + (p - 1)n^{p-2},
\]

\[
nF(n) = n + 2n^2 + \cdots + (p - 2)n^{p-2} + (p - 1)n^{p-1}.
\]

Hence \( (1-n)F(n) = (1 + n + n^2 + \cdots + n^{p-2}) - (p - 1)n^{p-1} \) and similarly

\[
(1-n)^2F(n) = 1 - n^{p-1} - (1-n)(p-1)n^{p-1} - 1 - p 
\cdot n^{p-1} + (p-1)n^p.
\]

Modulo \( p \), \( n^p = n \) by the Little Fermat Theorem and so \( (1-n)^2F(n) = 1 - n \). If neither \( a \) nor \( b \) is congruent to 1 (mod \( p \)), \( 1 - a \equiv 1 - b \) and there are distinct reciprocals \( (1 - a)^{-1} \) and \( (1 - b)^{-1} \) (mod \( p \)); then

\[
f(a) = (1 - a)^{-1}, f(b) = (1 - b)^{-1}, f(a) \equiv f(b) \pmod{p}.
\]

If one of \( a \) and \( b \), say \( a \), is congruent to 1, then \( b \equiv 0 \) (mod \( p \)) and so \( f(b) = (1 - b)^{-1} \equiv 0 \) (mod \( p \)) while

\[
f(a) = 1 + 2 + \cdots + (p - 1) = p(p - 1)/2 \equiv 0 \pmod{p}.
\]
A6. \((a_n)_{n \geq 1}\) is defined by \(a_1 = 1, a_2 = 2, a_3 = 24,\) and for \(n \geq 4,\)
\[
a_n = \frac{6a_{n-1}a_{n-3} - 8a_{n-1}^2a_{n-2}}{a_{n-2}a_{n-3}}.
\]
Show that, for all \(n,\) \(a_n\) is an integer multiple of \(n.\)

Solution. Rearranging the given equation yields the much more tractable equation
\[
\frac{a_n}{a_{n-1}} = 6 \frac{a_{n-1}}{a_{n-2}} - 8 \frac{a_{n-2}}{a_{n-3}}.
\]
Let \(b_n = a_n/a_{n-1}.\) With the initial conditions \(b_2 = 2, b_3 = 12,\) one obtains \(b_n = 2^{n-1}(2^{n-1} - 1),\) by induction or by the theory of linear recursive sequences: see the remark in 1988A5. Thus
\[
a_n = a_1b_2b_3 \ldots b_n = 2^{n(n-1)/2} \prod_{i=1}^{n-1} (2^i - 1).
\]

If \(n = 1,\) then \(n\) divides \(a_n.\) Otherwise factor \(n\) as \(2^k m,\) with \(m\) odd. Then \(k \leq n - 1 \leq n(n - 1)/2,\) and there exists \(i \leq n - 1\) such that \(m\) divides \(2^i - 1,\) namely \(i = \phi(m).\) (Here \(\phi\) denotes the Euler \(\phi\)-function: see 1985A4.) Hence \(n\) divides \(a_n\) for all \(n \geq 1.\)

Remark. Alternatively, the result for \(n \geq 3\) can be proved from the following two facts:

(a) The right side of the formula (1) for \(a_n\) equals \(2^{n-1} \# \text{GL}_{n-1}(\mathbb{F}_2).\) (See page xi for the definition of \(\text{GL}_{n-1}(\mathbb{F}_2).)\)

(b) If \(n \geq 3,\) \(\text{GL}_{n-1}(\mathbb{F}_2)\) contains an element of exact order \(n.\)

These suffice because of Lagrange's Theorem, which states that the order of an element of a finite group \(G\) divides the order of \(G.\)

Let us prove (a). Matrices in \(\text{GL}_{n-1}(\mathbb{F}_2)\) can be constructed one row at a time: the first row may be any nonzero vector, and then each successive row may be any vector not in the span of the previous rows, which by construction are independent. Hence the number of possibilities for the \(j\)th row, given the previous ones, is \(2^{n-1} - 2^{j-1}.\) Thus
\[
\# \text{GL}_{n-1}(\mathbb{F}_2) = \prod_{j=1}^{n-1} (2^{n-1} - 2^{j-1}) = 2^{(n-1)(n-2)/2} \prod_{j=1}^{n-1} (2^{n-j} - 1).
\]

Setting \(i = n - j\) and comparing with (1) proves (a).

It remains to prove (b). Let \(V = \{ (x_1, \ldots, x_n) \in (\mathbb{F}_2)^n : \sum x_i = 0 \}.\) Since \(\dim_{\mathbb{F}_2} V = n - 1,\) the group of automorphisms of the vector space \(V\) is isomorphic to \(\text{GL}_{n-1}(\mathbb{F}_2).\) Let \(T : V \to V\) be the automorphism \((x_1, x_2, \ldots, x_n) \mapsto (x_n, x_1, \ldots, x_{n-1}).\) Then \(T^n\) is the identity. If \(m < n\) and \(n \geq 3,\) then there exists \(v = (v_1, \ldots, v_n) \in V\) with \(v_1 = 1\) and \(v_{m+1} = 0:\) make just one other \(v_i\) equal to \(1,\) to make the sum zero. Then \(T^m v \neq v,\) so \(T^m\) is not the identity. Hence \(T\) has exact order \(n.\)

(The matrix of \(T\) with respect to the basis
\[
\epsilon_1 = (1, 1, 0, 0, \ldots, 0), \quad \epsilon_2 = (0, 1, 1, 0, \ldots, 0), \quad \ldots, \quad \epsilon_{n-1} = (0, 0, \ldots, 0, 1, 1)
\]
of \(V\) is
\[
\begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 1 \\
0 & 1 & 0 & \cdots & 0 & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 \\
0 & 0 & 0 & \cdots & 1 & 1
\end{pmatrix} \in \text{GL}_{n-1}(\mathbb{F}_2).
\]

This also equals the companion matrix of the polynomial
\[
f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1.
\]