PROBLEM SOLVER'S TOOLKIT

No. 9

Gerhard J. Woeginger

The Problem Solver's Toolkit contains short articles on topics of interest to problem solvers at all levels. Occasionally, these pieces will span several issues.

If it is not prime, it must be composite: part 2

Part 1 of this article appears on pages 409–412 of the previous issue (Volume 39, number 9).

3 Products of small numbers

No prime p divides a positive integer that is strictly smaller than p. Consequently: if we can show that a number q divides a product $f_1 f_2$ with $1 \leq f_1, f_2 < q$, then q must be composite. This trivial observation is surprisingly useful.

Problem 11 *Let a, b, c, d, e, f be positive integers, for which the sum $S = a+b+c+d+e+f$ divides both $Q = ab+ac+bc-de-df-ef$ and $R = abc+def$. Prove that S is composite.*

The occurrence of the terms $ab+ac+bc$, $de+df+ef$, abc and def in the problem statement urges us to consider the polynomial $P(x) = (x+a)(x+b)(x+c)-(x-d)(x-e)(x-f) = Sx^2+Qx+R$. Then S divides $P(x)$ for all integers x, and in particular S divides $P(d) = (a+d)(b+d)(c+d)$. As S is larger than each of the three factors, we conclude that S is composite.

Problem 12 *Consider the Fibonacci numbers defined by $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Prove that $F_n + 1$ is composite for all $n \geq 4$.*

The Fibonacci numbers satisfy the well-known Catalan identity $F_n^2 - F_{n-r}F_{n+r} = (-1)^{n-r}$. For odd n, we use $r = 1$ so that the identity becomes $(F_n+1)(F_n-1) = F_{n-1}F_{n+1}$. If $p = F_n + 1$ is prime, then it cannot divide the factor F_{n-1} which is smaller than p. But the other factor $F_{n+1} = F_n + F_{n-1}$ satisfies $p < F_{n+1} < 2p$, and hence cannot be divisible by p either. The argument for even n is very similar. We set $r = 2$ and use $(F_n+1)(F_n-1) = F_{n-2}F_{n+2}$. If $p = F_n + 1$ is prime, then the larger factor $F_{n+2} = 2F_n + F_{n-1}$ satisfies $2p < F_{n+2} < 3p$, and hence cannot be divisible by p. All in all, $F_n + 1$ must be composite.

The following three exercises can all be settled via products of small numbers.

Problem 13 *Let a, b, c, d be positive integers such that $a^2+ab+b^2 = c^2+cd+d^2$. Prove that $a+b+c+d$ is composite.*

Problem 14 *Let a, b, c be positive integers such that $a^2 - bc$ is a square. Prove that $2a+b+c$ is composite.*

Problem 15 *Let $a > b > c > d$ be positive integers with $a^2-ac+c^2 = b^2+bd+d^2$. Prove that $ab+cd$ is composite.*

4 Stepping stones

If you are stuck in a swamp of primes, you may sometimes use one of these primes as a stepping stone; you jump to a composite from it and reach the safe shore. The following folklore example illustrates this idea.

Problem 16 *Let $P(n)$ be a non-constant polynomial with integer coefficients. Prove that there exists an integer n for which $P(n)$ is composite.*

Pick an integer n for which $p = P(n)$ is prime as your stepping stone (if no such n exists, the proof is already complete). Consider the values $P(n+kp)$ for $k \geq 1$. As $(n+kp)-n$ divides $P(n+kp)-P(n)$, every such value $P(n+kp)$ is a multiple of p. But as the polynomial is non-constant, only a finite number of these infinitely many multiples can be equal to p. Hence you have successfully pulled yourself out of the swamp and jumped to a composite number $P(n+kp)$.

Problem 17 *Prove that the sequence $A(n) = n!^2 - n! + 1$ contains infinitely many composite numbers.*

Consider an odd integer $n \geq 3$ for which $p = A(n)$ is prime; note that $p > 2n+1$. This prime p will be our stepping stone. Since $k \equiv -(p-k) \bmod p$ holds for $1 \leq k \leq n$, we derive the following chain of equivalences modulo p:

$$\begin{aligned}(p-n-1)!\; n! &\equiv (p-n-1)! \cdot (p-n)(p-n+1)\cdots(p-2)(p-1)\cdot(-1)^n \\ &\equiv (p-1)!\cdot(-1)^n \equiv 1 \pmod{p}.\end{aligned}$$

In the last step of this chain, we have used Wilson's theorem together with the fact that n is odd. Next, we use this to show

$$\begin{aligned}n!^2 \cdot A(p-n-1) &\equiv n!^2\cdot(p-n-1)!^2 - n!^2\cdot(p-n-1)! + n!^2 \\ &\equiv 1 - n! + n!^2 \equiv A(n) \equiv 0 \pmod{p}.\end{aligned}$$

Since $n < p$, we conclude that p divides $A(p-n-1)$ and that $A(p-n-1)$ hence is composite. Now it is time to wrap things up: Whenever $A(n)$ is prime for some odd integer $n \geq 3$, then there exists another integer $m = p-n-1 > n$ for which $A(m)$ is composite. Hence the sequence indeed contains infinitely many composites.

We challenge the reader to settle the following problems along the lines indicated above.

Problem 18 *Let r and s be positive integers. Prove that the sequence $B(n) = r2^n + s3^n$ contains infinitely many composites.*

Problem 19 *Prove that there exist infinitely many odd integers n, for which $n!+1$ is composite.*

Problem 20 *Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a non-constant polynomial with integer coefficients. Prove that there exists a positive integer m for which $P(m!)$ is composite.*

Hints, comments, and references

11. This is problem N3 from the IMO 2005 shortlist, proposed by Mongolia.

13. Use $(b+c)(b+d) = (a+b+c+d)(c+d-a)$.

14. This is problem 1 from ELMO'2009, proposed by Evan O'Dorney. Let $a^2-bc = x^2$, and use $(2a+b+c)(2a-b-c) = (2x+b-c)(2x-b+c)$ with $a > x$.

15. This is problem 6 from IMO'2001, proposed by Aleksander Ivanov (Bulgaria). Show that $ab+cd > ac+bd > ad+bc$, and show that $ac+bd$ divides $(ab+cd)(ad+bc)$.

18. If $p = B(n)$ is prime with $p \notin \{2,3\}$, then $B(n+(p-1)k)$ is a multiple of p.

19. As n must be odd, Wilson does not help us here. Show that whenever $p = n!+1$ is prime for some odd $n \geq 3$, then p divides $(p-n-1)!+1$.

20. This is problem N7 from the IMO 2005 shortlist, proposed by Russia. Our problem 17 settles the special case with $P(x) = x^2 - x + 1$. The solution for the general case uses an additional trick: study the auxiliary polynomial $Q(x) = a_n + a_{n-1}x + \cdots + a_1 x^{n-1} + a_0 x^n$ and show that if a prime p divides $Q(m!)$ then p also divides $P((p-m-1)!)$.