PROBLEM SOLVER'S TOOLKIT

No. 8

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 1

There are a number of mathematical problems that ask for a proof that a given integer sequence contains at least one composite number, or that the sequence contains infinitely many composites, or that it entirely consists of composites. For instance, problem 96 in the book "250 Problems in Elementary Number Theory" by Wacław Sierpiński [2] asks: *"Does the sequence* 1*,* 31*,* 331*,* 3331*,* 33331*, ... contain infinitely many composite numbers?"* The answer turns out to be yes: the nth term of this sequence is $\frac{1}{3}(10^n - 7)$, and its 9th term is divisible by 17. A little bit of pondering then shows that for all $k \geq 1$ also its $(16k+9)$th term is divisible by 17.

In this 2-part article, we will survey several standard solution approaches to this problem type, and we will provide a multitude of illustrating examples. But first let us list a number of useful tools that we are going to apply throughout:

Difference of two powers. $a - b$ divides $a^n - b^n$ for integers a, b, n with $n \geq 1$.

Polynomial divisibility. $a - b$ divides $P(a) - P(b)$, for integers a and b and any polynomial $P(x)$ with integer coefficients.

Little Fermat. $n^{p-1} \equiv 1 \pmod{p}$ for a prime p and an integer n not divisible by p.

Wilson. $(p-1)! + 1 \equiv 0 \pmod{p}$ for every prime p.

Sophie Germain identity. $m^4 + 4n^4 = (m^2 + 2n^2 + 2mn)(m^2 + 2n^2 - 2mn)$

Fermat's theorem on sums of two squares. Every prime $p = 4k + 1$ can be written as sum of two squares in a unique way (up to the order of the two summands).

1 Proper divisors

There is a very simple and direct approach for proving that a given integer N is composite: exhibit a proper divisor of N. Of course, how to detect the *right*

proper divisor for settling a problem remains an art. The following two examples illustrate this approach.

Problem 1 *Show that $n^n + (n+1)^{n+1}$ is composite for infinitely many n.*

Let us analyze the auxiliary sequence n^n starting with 1, 4, 27, 256, 3125, 46656. Modulo 3 these six terms are $1, 1, 0, 1, 2, 0$, and it is not hard to see that this block of length 6 then repeats over and over again. Indeed, Fermat's little theorem implies $n^3 \equiv n \pmod 3$, and this yields $(n+6)^{n+6} \equiv n^{n+6} \equiv n^n \pmod 3$.

Now the solution of the problem has become straightforward: Pick $n = 6k+4$ so that $n^n \equiv 1 \pmod 3$ and $(n+1)^{n+1} \equiv 2 \pmod 3$, and use 3 as proper divisor.

Problem 2 *Let x and y be integers with $2 \le y < x \le 100$. Prove that there exists a positive integer n for which $x^{2^n} + y^{2^n}$ is composite.*

That's a baffling puzzle, primarily built around two crucial properties of the prime 257. The first crucial property is that $257 = 2^8 + 1$ is a power of 2 plus 1, and the second crucial property is that the only way of writing it as the sum of two squares is $257 = 16^2 + 1^2$. (Since $257 = 4 \cdot 64 + 1$, uniqueness follows from Fermat's theorem on sums of two squares.) Now note that

$$x^{256} - y^{256} = (x^{128} + y^{128})(x^{64} + y^{64}) \cdots\cdots (x^2 + y^2)(x + y)(x - y).$$

By Fermat's little theorem the left hand side is divisible by 257, so that one of the eight factors in the right hand side must be divisible by 257. As the two factors $x + y$ and $x - y$ are too small for this, there exists a positive integer n with $1 \le n \le 7$ such that $x^{2^n} + y^{2^n}$ is divisible by 257. Since x^{2^n} and y^{2^n} are squares and since $x, y > 1$, we conclude that $x^{2^n} + y^{2^n} \ne 257$. Hence this number $x^{2^n} + y^{2^n}$ is composite, as desired.

The reader may try to find the right divisors for the following exercises.

Problem 3 *Prove that there are infinitely many composites of the form (a) $10^n + 3$; (b) $(4^n + 1)^2 + 4$; (c) $n! - 1$.*

Problem 4 *Prove that there exist infinitely many integers n for which $2^n + 3^n - 4$ and $2^n + 3^n - 6$ are simultaneously composite.*

Problem 5 *Prove that for integers $n \ge 1$ each of the following numbers is composite: (a) $11 \cdot 14^n + 1$; (b) $19 \cdot 8^n + 17$; (c) $\frac{1}{3}(2^{2^{n+1}} + 2^{2^n} + 1)$.*

2 Factorizations

Another fundamental approach for proving that a given algebraic expression is composite is to write it as the product of two or more non-trivial factors. Here are two examples in which the factorizations are not straightforward to guess:

Problem 6 *Find all integers $n \ge 1$ for which $A(n) = n^4 + 4^n$ is prime.*

If n is even, then $A(n)$ is divisible by 4 and definitely not prime. If $n = 2k+1$ is odd, then $A(n) = n^4 + 4 \cdot (2^k)^4$. The Sophie Germain identity yields

$$A(n) \;=\; (n^2 + 2^{2k+1} + 2^{k+1}n)\,(n^2 + 2^{2k+1} - 2^{k+1}n).$$

For $n \geq 3$ both factors are greater than 1, so that $A(n)$ is composite. For $n = 1$ we get the prime $A(1) = 5$.

Problem 7 *Let a, b, c be positive integers with $3ab = 2c^2$. Show that $a^3 + b^3 + c^3$ is composite.*

The condition $3ab = 2c^2$ naturally causes one to consider the identity $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$. This then leads to

$$\begin{aligned} a^3 + b^3 + c^3 &= (a+b)^3 - 2c^2(a+b) + c^3 \\ &= (a+b)\left((a+b)^2 - c^2\right) + c^2(c-a-b) \\ &= (a+b-c)\,\left((a+b)(a+b+c) - c^2\right). \end{aligned}$$

The arithmetic-geometric mean inequality yields $a+b \geq 2\sqrt{ab} = 2\sqrt{2c^2/3} > c+1$. Hence both factors are greater than 1, and $a^3 + b^3 + c^3$ is composite.

Here are three exercises to test the reader.

Problem 8 *Find all integers n for which the following expressions are prime: (a) $n^4 + n^2 + 1$; (b) $n^{10} + n^5 + 1$; (c) $4n^3 + 6n^2 + 4n + 1$.*

Problem 9 *Let a, b, c, d be positive integers. Show that (a) $a+b+c+d$ is composite whenever $ab = cd$, (b) $a^2 + b^2 + c^2 + d^2$ is composite whenever $ad = b^2 + bc + c^2$.*

Problem 10 *Find all integers $n \geq 1$ for which $\frac{1}{5}(2^{4n+2} + 1)$ is prime.*

Hints, comments, and references

1. This is problem 19 from the 2012 Baltic Way competition.

2. This is problem 10.8 from the 2009 All-Russian Olympiad.

3. Parts (a) and (b) are problems 98 and 124 in Sierpiński [2].

(a) The terms with $n = 12k + 1$ are divisible by 13.

(b) The terms with $n = 28k + 1$ are divisible by 29.

(c) By Wilson's theorem, any prime p divides $(p-2)! - 1$.

4. For $n = 6k + 2$, the first number is divisible by 3 and the second number by 7.

5. Part (c) is problem 123 in Sierpiński [2]. The integers in the three parts are respectively divisible by one of (a) 3 and 5; (b) 3, 5, 13; (c) 7.

8. The terms in (a) and (b) have $n^2 + n + 1$ as a factor, and the term in (c) has $2n + 1$ as factor.

9. Part (a) is due to Olaf Krafft [1], and part (b) is from the 2nd round of the 2007 Polish Mathematical Olympiad.

(a) Use that $ab = cd$ implies that there are positive integers p, q, r, s with $a = pq$, $b = rs$, $c = pr$, and $d = qs$.

(b) Use that $a^2 + b^2 + c^2 + d^2$ can be rewritten as $(a + b + c + d)(a - b - c + d)$.

10. This is problem 99 in Sierpiński [2]. Use the Sophie Germain identity.

References

[1] O. Krafft (1983). Problem E3005. *American Mathematical Monthly 90*, 1983, 400.

[2] W. Sierpiński (1970). *"250 Problems in Elementary Number Theory"*. Polish Scientific Publishers, Warszawa.