Elementary Number Theory - Exercise 7a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Apply the Fermat and Solovay-Strassen primality tests to $n = 15$ with $a = 4$ and $a = 7$.

Problem 2. Show that 1105 is a Carmichael number.

Problem 3. Let n be a Carmichael number. Show the following results.

1. n must be odd. *Hint:* Find a suitable a violating Fermat's Little Theorem.
2. Each prime factor of n is smaller than $\sqrt{n}$. *Hint:* Show that $(p-1) \mid (\frac{n}{p} - 1)$.
3. n must have at least three different prime factors.
4. For primes p, q dividing n, we have $p \not\equiv 1 \pmod{q}$.

Problem 4. Prove the following rule due to Chernick, and use it to produce at least one Carmichael number:

If the three numbers $6k+1, 12k+1, 18k+1$ are prime, then their product

$$n = (6k+1)(12k+1)(18k+1)$$

is a Carmichael number.

Problem 5. Let G be a finite abelian group, with multiplication $\cdot$ and identity element 1. We define the *order* $\operatorname{ord}(g)$ of an element $g \in G$ as the smallest natural number m such that $g^m = 1$.

1. Show that, if $g^\ell = 1$ for some $\ell \in \mathbb{Z}$, then $\operatorname{ord}(g) \mid \ell$.
   Hint: Division with remainder.
2. G is called *cyclic* if there exists a $g \in G$ such that every element in G can be written as g^m for some $m \in \mathbb{Z}$. Each such g is called a *generator* of G. Show that G is cyclic if and only if it contains an element g of order $\operatorname{ord}(g) = |G|$.

Problem 6. Show that there exists a number $a \in \mathbb{Z}$ such that $\operatorname{ord}(a) = p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, deduce that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.
Hint: Let ℓ be the smallest positive number such that $a^\ell \equiv 1 \pmod{p}$ for all a with $\gcd(a, p) = 1$, and show that $\ell = p - 1$, using Fermat and Lagrange.

Problem 7 (sage)**.**

1. Implement the Fermat and Solovay-Strassen primality tests and apply them to 561.
2. Write a program that lists Carmichael numbers, and use it to find all Carmichael numbers $\leq 1.000.000$.