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 $a = 7$.

Solution 1. We first apply Fermat: we need to compute $a^{14} \pmod{15}$. For $a = 4$ we compute

$$4^{14} \equiv 16^7 \equiv 1^7 \equiv 1 \pmod{15}.$$

In particular, the Fermat test would output "15 is probably prime" with this choice of a. For $a = 7$ we compute

$$7^{14} \equiv 49^7 \equiv 4^7 \equiv 4 \cdot 4^6 \equiv 4 \cdot 16^3 \equiv 4 \cdot 1^3 \equiv 4 \pmod{15},$$

so the Fermat test will recognize that 15 is composite with this choice of a.

For the Solovay-Strassen test, we only consider $a = 4$, since we have seen for $a = 7$ we don't even have $a^{n-1} \equiv 1 \pmod{n}$, so we cannot have $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$. Now we need to compute $a^{\frac{n-1}{2}} \pmod{n}$. For $a = 4$ we compute

$$4^7 \equiv 4^6 \cdot 4 \equiv (16)^3 \cdot 4 \equiv 4 \pmod{15},$$

so the Solovay-Strassen test recognized that 15 is composite also on $a = 4$.

Problem 2. Show that 1105 is a Carmichael number.

Solution 2. We apply Korselt's criterion. The prime factorization is $1105 = 5 \cdot 13 \cdot 17$, so 1105 is square-free. Moreover, $4, 12$, and 16 all divide $1104 = 16 \cdot 3 \cdot 23$. Hence 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 $p \not\equiv 1 \pmod{q}$.

Solution 3.

1. If $n > 2$ is even, then $(-1)^{n-1} = -1 \neq 1 \pmod{n}$, so n is not a Carmichael number.
2. Let p be a prime factor of n. By Korselt's criterion, we also have $(p-1) \mid (n-1)$. Then

$$\frac{n-1}{p-1} = \frac{(p \cdot \frac{n}{p} - 1)}{p-1} = \frac{(p-1)\frac{n}{p} + \frac{n}{p} - 1}{p-1} = \frac{n}{p} + \frac{\frac{n}{p} - 1}{p-1},$$

so $(p-1) \mid (\frac{n}{p} - 1)$. In particular $p \leq \frac{n}{p}$. Since equality could only occur if $n = p^2$, but Carmichael numbers are square-free, we find $p < \frac{n}{p}$, so $p < \sqrt{n}$.

3. If n had only two prime factors, $n = pq$ (recall that Carmichael numbers are composite and square-free), then by the last item we would have $n = pq < \sqrt{n}\sqrt{n} = n$, which is a contradiction.

4. Let p, q be prime factors of n and assume that $p \equiv 1 \pmod{q}$. Then $q \mid (p-1) \mid (n-1)$ by Korselt's criterion, which is impossible since $q \mid n$.

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.

Solution 4. We apply Korselt's criterion. By assumption, n is a product of three different primes $p_1 = 6k+1, p_2 = 12k+1, p_3 = 18k+1$. In particular, n is composite and square-free. We need to show that $6k, 12k, 18k$ divide $n-1$. Modulo $12k$, we have

$$n \equiv (6k+1)(12k+1)(18k+1) \equiv (6k+1)(6k+1) \equiv 36k^2 + 12k + 1 \equiv 12k,$$

which implies that $6k$ and $12k$ divide $n-1$. Modulo $18k$ we have

$$n \equiv (6k+1)(12k+1)(18k+1) \equiv (6k+1)(12k+1) = 72k^2 + 18k + 1 \equiv 1 \equiv 18k,$$

which implies that $18k$ divides $n-1$. By Koreslt's criterion, n is a Carmichael number.

For example, for $k = 1$ we obtain the three primes $7, 13, 19$, and their product

$$n = 7 \cdot 13 \cdot 19 = 1729$$

is a Carmichael number. For $k \leq 10$ the only other case in which all three numbers are prime is $k = 6$, in which case we get the Carmichael number

$$n = 37 \cdot 73 \cdot 109 = 294409.$$

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 $\operatorname{ord}(g) = |G|$.

Solution 5. 1. Suppose that $g^\ell = 1$. We divide ℓ by $\operatorname{ord}(g)$ with remainder,

$$\ell = q\operatorname{ord}(g) + r, \quad 0 \leq r < \operatorname{ord}(g),$$

to find

$$g^r = g^{\ell - q\operatorname{ord}(g)} = 1.$$

Since $r < \operatorname{ord}(g)$ and $\operatorname{ord}(g)$ is the smallest positive number with $g^m = 1$, we must have $r = 0$. Hence, $\ell = q\operatorname{ord}(g)$, so ℓ is divisible by $\operatorname{ord}(g)$.

2. For any $g \in G$, the set of powers of g,

$$\langle g \rangle = \{g^m : m \in \mathbb{Z}\},$$

that is, the *subgroup generated by* g, contains precisely $\mathrm{ord}(g)$ elements, namely

$$\langle g \rangle = \{g, g^2, g^3, \dots, g^{\mathrm{ord}(g)} = 1\}.$$

This can also be checked rigorously using division with remainder as in the last item. In particular, if $\mathrm{ord}(g) < |G|$ for every $g \in G$, then $\langle g \rangle$ contains less elements than G, so we cannot write every element in the form g^m, and G is not cyclic. However, if $\mathrm{ord}(g) = |G|$ for some $g \in G$, then $\langle g \rangle$ is a subset (even a subgroup) of G with the same number of elements, so $\langle g \rangle = G$, which means that G is cyclic.

Problem 6. Show that there exists a number $a \in \mathbb{Z}$ such that $\mathrm{ord}(a) = p - 1$ 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.

Solution 6. Let ℓ be the smallest positive number such that $a^\ell \equiv 1 \pmod p$ for all a with $\gcd(a, p) = 1$. We want to show that $\ell = p - 1$. Fermat's Little Theorem implies that $\ell \leq p - 1$. On the other hand, by the choice of ℓ, the polynomial $x^\ell - 1$ has $p - 1$ roots in $\mathbb{Z}/p\mathbb{Z}$, so by Lagrange's Theorem, its degree ℓ must be at least $p - 1$, i.e. $\ell \geq p - 1$. This shows $\ell = p - 1$. Hence, there exists some a with $a^\ell \neq 1 \pmod p$ for all $\ell < p - 1$, which means that $\mathrm{ord}(a) = p - 1$.

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 $\leq 1.000.000$.