Math 55 - Section
Homework 7
Thursday, November 3, 2016

1, 2, 3, 4, 5, 6, 7

**1** Consider the recursive algorithm described in class for exponentiation, computing

$$a^n \pmod{m},$$

where the exponent $n$ is halved, or reduced by one, at each step.

(a) How many multiplications (and reductions modulo $m$) does this algorithm use when $n = 15$?

(b) Find a way of computing $a^{15} \pmod{m}$ that uses fewer multiplications (and reductions modulo $m$) than in part (a).

(Hint: $15 = 3 \cdot 5$.)

∎

**2** When doing modular exponentiation modulo $m$, if $a$ is relatively prime to $m$, it is possible to divide by powers of $a$, in addition to multiplying them.

(a) How many multiplications (and reductions modulo $m$) does the algorithm described in class use when $n = 31$?

(b) Find a way of computing $a^{31} \pmod{m}$ that uses fewer multiplications and divisions (and reductions modulo $m$) than in part (a).

■

**3** Show that there are infinitely many primes of the form $4k + 3$.

(Hint: Consider the number $N = 2^2 p_3 \cdots p_k + 3$. Note that two odd numbers of the same "type" mod 4 (both 1 or both 3) have a product that is 1 mod 4, whereas two odd numbers of opposite type have a product that is 3 mod 4.)

■

**4** Show that $n = 1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number (that is, that even though $n$ is not prime, it satisfies

$$a^{n-1} \equiv_n 1$$

for all $a$ relatively prime to $n$).

∎

**5** How many different solutions to the congruence

$$x^2 \equiv 1 \pmod{1729}$$

are there?

(Here "different" means different modulo $1729 = 7 \cdot 13 \cdot 19$. Give a concise justification for your answer, not a brute-force search.)

■

**6** Say that a positive integer $t$ is *square-free* if it is not divisible by any square other than 1. Show that every positive integer $n \geq 1$ can be written in a unique way as $n = xy$, where $x$ is a square and $y$ is square free.

■

**7** Show that if $m_1, \ldots, m_k$ are pairwise relatively prime, then the congruences

$$x \equiv_{m_1} a_1, \ \ldots, \ x \equiv_{m_k} a_k$$

have a solution that is unique modulo $m_1 \cdots m_k$.

(You may use the case $k = 2$, which is the Chinese remainder theorem.)

∎