Mathematics 360 **Final (100 points)** Due 12/20/13, 9:30am

Points (leave blank)								
1	2	3	4	5	6	7	8	∑

Name:

(clearly, please)

This exam is my own work. Sources (apart from the textbook and material available on the course web page) are indicated. I have not given, received, or used any unauthorized assistance.

Signature

This final is due at the leatest Friday, December 20 2013 at 9.30am (at my office or in my mailbox).

Notes

- Put your name on this cover sheet and sign it.
- All problems carry the same credit, you may work on them in any order you like.
- You have no time limit (beyond the due date) for working on the exam. (However the exam was posed so that with a computer being available for arithmetic it can be done in 2 hours.)
- You are permitted to use your notes and any publication (book, journal, web page). You are not permitted to consult third persons.
  Results which are quoted from a publication (apart from the course textbook or material on the corse web page) should be indicated.
- You may assume that all assertions in a problem (e.g. about numbers being prime or about a prime factorization of number) are true unless the problem explicitly asks to show it.
- Unless specified otherwise, you may use a computer for arithmetic (including the extended Euclidean algorithm) as well as for initial exploration.

  Computer commands, which render the problem trivial (for example using factorization to show that a number is prime), however are not considered a sufficient solution.
- A complete solution contains the calculations that were done (either by hand, or by indicating the computer commands used).
- If a problem specifies that the solution is to be done in a particular way, no points will be given if the problem solved in a different way.
- If you need extra sheets, staple them to this final. (You do not need to submit scrap paper that has no grade value.)
- I will post exam scores and final grades on RamCT by December 24, you may pick up you graded final exam in the mathematics front office in 2014.

1) A message a has been encrypted using the RSA public key modulus $n = 2550306041$ and exponent $e = 5$. The encrypted message is $c = 1176337529$. Your computer has found that 33343 is a factor of n. Decrypt the message.

2) The number $p = 2311 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$ is prime.
a) How many primitive roots modulo p exist?
b) You are given the information that $g = 3$ is a primitive root mod p. Without searching through all numbers, find one exponent e such that $\mathrm{OrderMod}_p(g^e) = 35$ and two exponents e_1, e_2 such that $\mathrm{OrderMod}_p(g^{e_i}) = 105$.

3) a) Using the Miller-Rabin test, show that 1033 is prime with error probability less than 1%.
b) Using the Miller-Rabin test, show that 1037 is not prime.
c) Find a factor of 1037 using the Pollard-ρ factorization algorithm. (If you want, you may select to simply form all differences rather than to use the cycle-detection mechanism. You also don't have to reduce the number of GCD calculations.)

4) (Chinese Remainder Theorem)

The Organization Without a Cool Acronym (OWCA) maintains a black safe for emergencies. Its key is a large number k.

It now wants to set up a scheme such that any two agents will be able to open the safe if necessary, but no single agent should be able to do so. (Agents have their mind wiped after opening the safe so that they do not remember information about the key k afterwards.)

For this purpose, it assigns each agent a number m_i (these numbers m_i are public knowledge) and gives the (secret) information $k \bmod m_i$ to agent number i.

a) How can you choose the m_i so that any two cashiers can determine k but each cashier still would have many possible values of k to try?

b) Assume (small example) that $k = 12345$. Construct such a set $\{m_1, \ldots, m_5\}$ for 5 agents.

5) Let $p = 1297 = 2^4 3^4 + 1$ (which is prime). Then $r = 10$ is a primitive root modulo p. Determine e such that $10^e \equiv 657 \pmod{p}$ using the methods known from class. If you decide to use a Baby-step/Giant-step algorithm, your lists should not have more than 4 elements (i.e. you may use Baby-step/Giant-step, or an explicit list, for exponents up to 16, should you desire to do so).

6) You are asked for advice on the selection of a public key for RSA encryption (in practice the numbers would be much larger, but for simplicity this problem is scaled down. Also you should ignore the computational cost of encryption/decryption). Which set of the following number pairs (n, e) should be chosen to ensure secure encryption? Explain your choice. (**Hint:** All keys but one are flawed. You might for example want to go through the process of determining decryption keys to see why.)

$$
\begin{aligned}
n &= 365413900459 = 2081 \cdot 175595339, & e &= 33 \\
n &= 151560550847 = 270133 \cdot 561059, & e &= 6314988319 \\
n &= 550887536183 = 821329 \cdot 670727, & e &= 462500158037 \\
n &= 165940048999 = 219757 \cdot 755107, & e &= 45306361 \\
n &= 200052807277 = 633317 \cdot 315881, & e &= 133367905387
\end{aligned}
$$

7) a) Suppose that r is a primitive root modulo $n > 2$. Using that $-1^2 = 1$, show that $\mathrm{OrderMod}_n(r)$ must be even.
b) Let $n = a{\cdot}b$ odd with $\gcd(a, b) = 1$. Show, using the Chinese Remainder Theorem, that $\mathrm{OrderMod}_n(x) = \mathrm{lcm}(\mathrm{OrderMod}_a(x), \mathrm{OrderMod}_b(x))$ for x with $\gcd(x, n) = 1$. (We've done this briefly in class. You may consult your notes but should give a full, self-contained, proof here.)
c) Again consider $n = a \cdot b$ odd with $\gcd(a, b) = 1$, thus $\varphi(n) = \varphi(a) \cdot \varphi(b)$. Conclude from a),b) that there is no primitive root modulo n.

8) Santa is sending a message to the Elves. He has encrypted it using a Vigenère cipher with keyword TREE. Decrypt it:

ARTTR YSPBU ECL

(Note: If you get a text starting with TI you are accidentally *encrypting* again, not decrypting.)