Mathematics 400c **Final (126+12 points)** Due 5/11/02, 3.30pm

Points (leave blank)												
1	2	3	4	5	6	7	8	9	10	11	12	$\sum$

Name:

(clearly, please)

This exam is my own work. Sources (apart from the textbooks and my lecture notes) are indicated.

_____

Signature

This final is due Tuesday, May 11th 2004 at 3.30pm (at my office or in my mailbox).

Notes

- Put your name on this cover sheet and sign it.
- 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 textbooks and your lecture notes) should be indicated.
- Unless specified otherwise, you may use a computer for arithmetic (including extended Euclidean algorithm, power modulo and – unless this is the main task of the problem – factorization) 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 you need extra sheets, staple them to this final. (You do not need to submit scrap paper.)
- I hope to have grades posted by Friday. You can pick up your exam (and obtain your grade) from me on Friday, May 15, between 11 am and 12 am at my office (or a later time by appointment).

1) Find by hand all solutions to the following congruences:

a) $3x + 5 \equiv 7 \pmod{23}$

b) $9x \equiv 14 \pmod{24}$

c) $9x \equiv 15 \pmod{24}$

(12 points)

2) Determine all n for which $\phi(n) = 2p^2$ with $p > 2$ prime. **(8 points)**

3) a) Show that if $p \equiv 1 \pmod 4$ and g is a primitive root mod p that also $-g$ is a primitive root mod p.
b) Give an example that shows that the claim in a) fails if $p \equiv 3 \pmod 4$. **(8 points)**

4) Determine (without using a `ChineseRem` function) a solution to the following set of congruences:

$$\begin{aligned} x &\equiv 2 \pmod{27} \\ x &\equiv 4 \pmod{8} \\ x &\equiv 7 \pmod{25} \end{aligned}$$

(8 points)

5) The number $p = 211$ is prime. How many primitive roots modulo p exist? You are given the information that $g = 2$ is a primitive root mod p. Determine (without exhaustively testing all numbers) all e, such that g^e is a primitive root mod p. **(12 points)**

6) We are calculating modulo $p = 347$, which is a prime modulus.
a) Show that 2 is a primitive root mod p.
b) Calculate $\mathrm{ind}_2(78)$ and $\mathrm{ind}_2(32)$.
c) Determine an x such that $78^x \equiv 32 \pmod{347}$. **(12 points)**

7) a) Let $k < n$ be positive integers with $\gcd(k, \varphi(n)) = 1$. Show that there is an integer e such that for all a with $\gcd(a, n) = 1$ the congruence $x^k \equiv a \pmod{n}$ has the unique solution $x = a^e$.
b) For $n = 16349253 = 3 \cdot 19 \cdot 97 \cdot 2957$, solve the congruence $x^7 \equiv 13470 \pmod{n}$.
(12 points)

8) a) In how many ways can $3205556521 = 89 \cdot 211^2 \cdot 809$ be written as a sum of two squares?
b) Determine (without exhaustively searching through all pairs of numbers) the different ways, in which 3205556521 can be written as a sum of two squares. **(15 points)**

9) Using the Quadratic Reciprocity Law, determine whether the following equations have a solution (You may assume that all moduli are prime). you do not need to give the solutions:

a) $x^2 \equiv 19 \pmod{5737}$

b) $x^2 \equiv 18 \pmod{5737}$

c) $x^2 + 3x + 17 \equiv 0 \pmod{5737}$

(12 points)

10) We want to factorize 1871369 with the quadratic sieve.
a) Determine all primes smaller than 40 which can be factors of $x^2 - n$.
b) Write down a sieving table for a factor base given by the primes in a), and a sieving interval of length $2 \cdot 20$.
c) Factorize 1871369 with the quadratic sieve. (You may assume that the number is the product of 2 primes.)
: Note: You might end up with two equal numbers x and y (and thus not get a proper factor). This is an acceptable result. (15 points)

11) a) Using a strong pseudoprime test, verify which of the following numbers are prime:

$$118901509, \quad 118901517, \quad 118901521$$

b) For the numbers in a) that are prime, give a certificate of their primality. You may assume knowledge of all primes ≤ 50 and may use the computer to factor $n-1$. (12 points)

12*) We consider numbers in the set $A = \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Show that if $3 = \alpha \cdot \beta$ with $\alpha, \beta \in A$, we must have that $\alpha = \pm 1$ or $\beta = \pm 1$.
(Hint: Define a suitable norm function and show that it is multiplicative.) (12 points)