North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

**Department of Mathematics**

NC STATE UNIVERSITY

MA 410 Theory of Numbers, final examination, May 1, 2009
Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring09/ (URL)

919.515.8785 (phone)
919.515.3798 (fax)



*Your Name:* SOLUTION
For purpose of anonymous grading, please do **not** write your name on the subsequent pages.

This examination consists of 6 problems, which are subdivided into 11 questions, where each question counts for the explicitly given number of points, adding to a total of **46 points**. Please write your answers in the spaces indicated, or below the questions, using the **back of the sheets** for completing the answers and **for all scratch work,** if necessary. You are allowed to consult **three** 8.5in $\times$ 11in sheets with notes, but **not** your book or your class notes. If you get stuck on a problem, it may be advisable to go to another problem and come back to that one later.

You will have **120 minutes** to do this test.

Good luck!

| | |
|---|---|
| Problem 1 | ____ |
| 2 | ____ |
| 3 | ____ |
| 4 | ____ |
| 5 | ____ |
| Total | ____ |

**Problem 1** (16 points)

(a, 4pts) What makes a public key cryptosystem public? Please explain by example of the RSA.

*Everyone knows how messages are encrypted. For the RSA, the encryption algorithm computes for a message M the cipher* $M^E \bmod K$ *where E and K are publicly known integers.*

(b, 4pts) True of false: For all integers $x, y, z, k$ with $xyz \neq 0$ and $k \geq 2$ we have $x^{2^k} + y^{2^k} \neq z^2$. Please explain your answer.

*True: this is a special case of Fermat's theorem:* $(x^{2^{k-2}})^4 + (y^{2^{k-2}})^4 \neq z^2$.

(c, 4pts) Please prove: let $p > 2$ be a prime number such that $p \equiv 3 \pmod 4$, i.e., $p - 1$ is a quadratic non-residue. Then for all $x, y \in \mathbb{Z}_p$ with $x > 0, y > 0$ one has $x^2 + y^2 \not\equiv 0 \pmod p$.

*Suppose there are such residues* $x, y$*: then* $-1 \equiv (xy^{-1})^2 \pmod p$*, hence a quadratic residue. But* $(-1)^{(p-1)/2} \equiv -1$*, so* $-1$ *is a QNR modulo* $p$*.*

(d, 4pts) True of false: there does **not** exist an algorithm that for a system of polynomial equations with integer coefficients determines if the system has a solution where the values of the variables are integers.

*True: this is a famous theorem proven in the 1960s.*

**Problem 2** (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{110}{199}\right)$. Please show all your work.

$\left(\frac{110}{199}\right) = \left(\frac{2}{199}\right)\left(\frac{55}{199}\right) = (-1)^{\frac{199^2-1}{8}}\left(\frac{55}{199}\right) = +\left(\frac{55}{199}\right)$
$\left(\frac{55}{199}\right) \cdot \left(\frac{199}{55}\right) = (-1)^{\frac{55-1}{2}\cdot\frac{199-1}{2}} = -1,$
$\left(\frac{199}{55}\right) = \left(\frac{34}{55}\right) = \left(\frac{2}{55}\right)\left(\frac{17}{55}\right) = +\left(\frac{17}{55}\right)$, $\left(\frac{17}{55}\right) \cdot \left(\frac{55}{17}\right) = (-1)^{\frac{55-1}{2}\cdot\frac{17-1}{2}} = +1$
$\left(\frac{55}{17}\right) = \left(\frac{4}{7}\right) = +1 \Longrightarrow \left(\frac{110}{199}\right) = -1.$

**Problem 3** (5 points): Let $p > 2$ be a prime integer with $p \equiv 5 \pmod 8$, and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo $p$ with $a^{(p-1)/4} \equiv -1 \pmod p$. Please explain how you can compute a residue $b$ with $b^2 \equiv a \pmod p$.

*Select a quadratic non-residue* $c \in \mathbb{Z}_p$ *by randomly testing* $c^{\frac{p-1}{2}} \equiv -1 \pmod p$. *Then set* $b = (a^{\frac{p+3}{8}} c^{\frac{p-1}{4}} \bmod p)$. *then* $b^2 \equiv a^{\frac{p-1}{4}} c^{\frac{p-1}{2}} a \equiv a \pmod p$.

**Problem 4** (15 points): Consider the following table of indices (discrete logarithms) for the prime number 19 with respect to the primitive root $g = 2$:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{ind}_2(a)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

(a, 5pts) By inspecting the above table, for the multiplicative orders $k = 1, 2, 3, 6, 9, 18$ please list one residue $a_k \in \mathbb{Z}_{19}$ each that has order $k$ (belongs to the exponent $k$ modulo 19).

*a has order k* $\Longleftrightarrow a = g^i$ *with* $\gcd(i, 18) = 18/k$.
*So* $a_1 = 2^{18} = 1, a_2 = 2^9 = 18, a_3 = 2^6 = 7, a_6 = 2^3 = 8, a_9 = 2^2 = 4, a_{18} = 2$.

(b, 5pts) Using the above table, please solve $x \in \mathbb{Z}_{19}$ and all $y \in \mathbb{Z}_{19}$ the two congruences

$$x^4 \equiv 5 \pmod{19}, \quad 7y^7 \equiv 8 \pmod{19}$$

Please give all solutions and show your work.

$5 \equiv 2^{16} \pmod{19}$
$4 \cdot ind(x) \equiv 16 \pmod{18}$, $2 \cdot ind(x) \equiv 8 \pmod{9}$, $ind(x) \equiv 4 \pmod{9}$, $ind(x) = 4$ *and* $ind(x) = 13$,
$x_1 = 16, x_3 = 3$.

$7 \cdot ind_2(y) + ind_2(7) \equiv ind_2(8) \pmod{18}$,
$ind_2(y) \equiv 7^{-1}(3-6) \equiv 15 \pmod{18}$ *(by extended Euclidean algorithm not shown), so* $y = 12$.

(c, 5pts) Suppose Alice has digitally signed her signature $F_A \in \mathbb{Z}_{19}$ by the el-Gamal public key system. The shared modulus is $p = 19$ and the shared primitive root is $g = 2$. Her public key is $h_A = 15 \equiv 2^{s_A} \mod 19$. Her digital signature using Bob's $x_B = 9 \equiv 2^{r_B} \mod 19$ is $G_A = 10 \in \mathbb{Z}_{19}$. Please show how Bob computes $F_A$. You can use the table in part (a) to determine Bob's secret random exponent $r_B$, but not Alice's private key, namely exponent $s_A$.

$r_B = 8$
*Bob encrypts $G_A$ as the pair $x_B$ and $F_A = y_B = (G_A h_A^{r_B} \mod 19) = 10 \cdot 15^8 \mod 19 = 12$.*

**Problem 5** (5 points): Please find three **relatively prime** integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^2 + y^6 = z^2$. Please show your work.

*$y = 2st$, so we can choose $s = 4$ and $t = 1$. Thus $x = s^2 - t^2 = 15$, $y = 2$, and $z = s^2 + t^2 = 17$.*