NC STATE UNIVERSITY

MA 410 Theory of Numbers, final examination, May 1, 2009 Prof. Erich Kaltofen <pre><kaltofen@math.ncsu.edu></kaltofen@math.ncsu.edu></pre> www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spr © Erich Kaltofen 2009	ing09/(URL)	919.515.8785 (phone) 919.515.3798 (fax)								
Your Name:										
For purpose of anonymous grading, please do not v	write your name on the subs	equent 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 8.5 in \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										
4										
5										
Total										

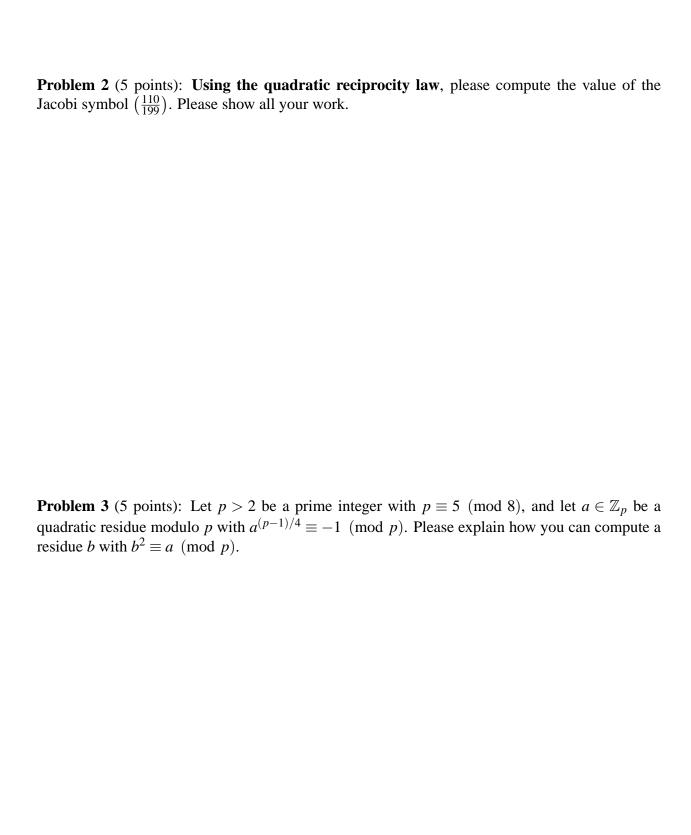
Problem 1 (16 points)

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

(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.

(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 $x^2 + y^2 \not\equiv 0 \pmod p$.

(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.



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:

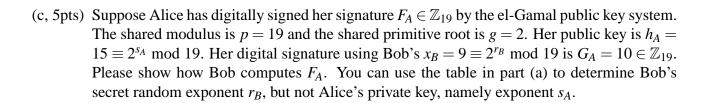
а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$ind_2(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(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).

(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.



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.