Final exam
The exam is due Monday May 12, before 3:45PM
(See you e-mail for details)

The use of mathematical software is not allowed, though you can use simple calculators. To get a full credit you should justify your answers and show all the work.

1. Determine how the number of solutions of the congruence \( x^2 + x + 1 \equiv 0 \mod p \) depends on \( p \).

2. Determine the number of solutions of the equation \( \phi(n) = 30 \).

3. Evaluate \( <4,1,2,1,8> \).

4. Find all integral solutions of \( x^2 - 9y^2 = 4 \).

5. Find all rational solutions of \( 7x^2 - y^2 = -1 \).

6. Find all invertible elements in \( \mathbb{Z}[\sqrt{3}] \).

7. Which of the following statements true or false (construct supportive examples where necessary):
   a. There is an irreducible monic quadratic polynomial \( Q(x) \in \mathbb{Z}[x] \) such that its reduction mod \( p \) for some \( p \) is an irreducible polynomial \( q(x) \in \mathbb{Z}_p[x] \).
   b. There is an irreducible monic quadratic polynomial \( Q(x) \in \mathbb{Z}[x] \) such that its reduction mod \( p \) for all \( p \) is an irreducible polynomial in \( \mathbb{Z}_p[x] \).
   c. Any irreducible monic quadratic polynomial \( q(x) \in \mathbb{Z}_p[x] \) is a reduction of an irreducible \( Q(x) \in \mathbb{Z}[x] \).
   d. There is a reducible monic quadratic polynomial \( q(x) \in \mathbb{Z}_p[x] \) such that it is a reduction mod \( p \) of an irreducible monic quadratic polynomial \( Q(x) \in \mathbb{Z}[x] \).
8. Prove that \((2^{2k+1} - 1, 2^n + 1) = 1\) for all positive \(k, n\).

9. Decode the message \(C = 3095\) if the public key is \(n = 2173\) (the base), \(e = 361\) (the exponent). **Show all the work.**

10. We suppose that three senders are using different integers \(n_1, n_2, n_3\), but using the same exponent \(e_1 = e_2 = e_3 = 3\). Show that if these three senders encrypt the same message \(P\) (thus producing three public encrypted messages \(C_i \equiv P^3 \mod n_i\)), then one can recover the initial message \(P\).