CS 4031 **April, 2017**

Computational Algebra **Final Exam** **36 Marks**

1. Let $p = 43$. Let $a \neq \pm 1$, $a \in Z_p^*$ be a quadratic residue. Find a positive integer k such that a^k is a square root of a mod p. Justify your answer. [3]

   Soln: Let $k = \frac{p+1}{4}$. Then $(a^k)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}}.a = 1.a = a \mod p$. Thus $k = 11$ solves.

2. Let p be a prime number of the form $4k+3$. Is it always true that a is a quadratic residue if and only if $-a$ is a quadratic non-residue. (Hint: Carefully observe calculations of the previous question!). [3]

   Soln: if a is a quadratic non-residue then $a^{\frac{p-1}{2}} = -1$. Hence, $(a^{\frac{p+1}{4}})^2 = -a$. Thus $-a$ is a quadratic residue. Conversely, if a is a quadratic residue, then $(-a)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}.(-1)^{\frac{p-1}{2}} = -1$ (why?). Hence $-a$ is a quadratic non-residue.

3. Find all values of $a \in Z_{17}^*$ such that $a^{\frac{n-1}{2}} \mod 17 \neq \left(\frac{a}{17}\right)$ [3]

   Soln: This question was set as an easy "take away".

4. Let $n = p^k m$, $k \geq 2$ with $GCD(m,p) = 1$, $m > 1$ odd. Let g be a generator of $Z_{p^2}^*$. Let $a \equiv g \mod p^k$ and $a \equiv 1 \mod m$. Is it true that $a^{\frac{n-1}{2}} \mod n \neq \left(\frac{a}{n}\right)$? Prove/disprove. [3]

   Soln: $a = (g,1) \in \mathbf{Z}_{p^k}^* \times \mathbf{Z_m}^*$. Now $a^{\frac{n-1}{2}} = (g^{\frac{n-1}{2}} \mod p^k, 1) \in \mathbf{Z}_{p^k}^* \times \mathbf{Z}_m^*$. On the other hand $\left(\frac{a}{n}\right)$ can assume values only ± 1. Consequently, equality between the two is possible if and only if $g^{\frac{n-1}{2}} \mod p^k = 1$ (why?). But this would imply that $g^{\frac{n-1}{2}} = 1 \mod p^2$. But then $o(g)$ in $\mathbf{Z}_{p^2}^*$ must divide $\frac{n-1}{2}$ (Lagrange), This would imply that $p(p-1)$ must divide $\frac{n-1}{2}$ and thus p must divide $n-1$, a contradiction as p can't divide both n (as originally assumed) as well as $n-1$.

5. Let r be randomly chosen from Z_n^* for a given n satisfying conditions of the previous question. Suppose we announce n composite if and only if $r^{\frac{n-1}{2}} \mod n \neq \left(\frac{r}{n}\right)$, can we say that the test announces n composite with probablity at least $\frac{1}{2}$? - prove/disprove. [3]

   Soln: Let $S_n = \{a \in \mathbf{Z}_n^* : a^{\frac{n-1}{2}} \mod n \equiv \left(\frac{a}{n}\right) \mod n\}$. It is easy to see that S_n is a subgroup of $\mathbf{Z}_n^*$ and that $a \in \mathbf{Z}_n^*$ fails the test if and only if $a \in S_n$. Thus, if S_n is a proper subgroup of $\mathbf{Z}_n^*$, the test announces n composite with probability at least $\frac{1}{2}$ (why?- Largrange). In the previous question we have seen the existance of one element outside S_n. Hence, S_n is indeed a proper subgroup of $\mathbf{Z}_n^*$.

6. Let $n = p_1 p_2 .. p_k$ be a Carmichael number. Prove that there exists $a \in Z_n^*$ such that $a^{\frac{n-1}{2^k}} \neq -1$ for all $k \geq 1$ such that 2^k divides $(n-1)$. [3]

   Soln: This question is easier than it was designed to be. Simply setting $a = 1$ solves! unfortunately(?) - I missed putting the condition $a \neq 1$ in the question. Even if the condition was there, you could have found such a as follows: pick a such that $a = -1 \mod p_1$ and $a \equiv 1 \mod p_i$, $1 < i \leq k$. No power of this element can be equal to -1 (why?).

7. What will Miller Rabin test return if a is the randomly chosen element for testing compositeness of n, a, n satisfying conditions stated in the previous question? Justify your answer. [3]

   Soln: Let $n - 1 = 2^k m$, m odd. If $a^m \neq \pm 1$ Miller Rabin will return COMPOSITE; otherwise, Miller Rabin will return PRIME. The reasoning is left to you.

8. Let (b_1, b_2) be a basis for a (two dimensional) lattice $\mathcal{L}$ with $||b_1|| \leq ||b_2|| \leq ||b_2 + qb_1||$ for all $q \in \mathbf{Z}$. Prove that $||v|| \geq ||b_2||$ for all $v \in \mathcal{L}$, $v \notin Span(b_1)$. (Answer on the reverse side). [3]

   Soln: See http://athena.nitc.ac.in/~kmurali/Courses/17CompAlgebra/gauss.pdf for a proof.

9. Let (b_1, b_2) be a basis for a (two dimensional) lattice $\mathcal{L}$ with $||b_1|| = ||b_2||$. Can we conclude that (b_1, b_2) is a reduced basis for $\mathcal{L}$? Prove / Provide counter example. [3]

   Soln: Consider $b_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $b_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$. It is easy to see that $b_1 - b_2$, is a vector in the lattice shorter than both.

10. A prime number of the form $p = 2^k + 1$ for some positive integer k is called a **Fermat Prime**. (Ex: 3,5,17). Show that if $2^k + 1$ is prime, then k must be a power of 2. (That is $p = 2^{2^r} + 1$ for some $r \geq 0$.). Hint: When m is odd, $(a + b)$ is a divisor of $(a^m + b^m)$. [3]

    Soln: Consider a Fermat prime p of the form $2^{2^t m} + 1$ with m odd. Put $x = 2^{2^t}$. Then $p = x^m + 1$. Hence $(x + 1)$ must be a divisor of p. As p is prime, m must be 1.

11. Consider the following four step algorithm that is claimed to test whether a given n is a Fermat prime: 1. if $(n-1)$ is not a power of 2, return NO. 2. Randomly chose $a \in \{1, 2, ..(n-1)\}$. 3. if $a^{\frac{n-1}{2}} = 1$ return NO. 4. Return YES. [3+3]

    1. Derive an upper bound on the probability that the algorithm announces NO if n is actually a Fermat prime?
    2. What is the (worst case) probability that the algorithm announces YES when n is not prime?

    Soln:

    1. Let p be a Fermat prime. Let $p - 1 = 2^t$. Since Z_p^* is cyclic of order $\phi(p-1) = 2^{t-1} = \frac{\phi(p)}{2}$, with probability $\frac{1}{2}$, a random element $a \in Z_p^*$ is a generator of Z_p^*, and for such a, the algorithm will not return NO in Step 2 (and hence return YES). (why?).
    2. If the random element is 1 or -1, clearly the test will return NO except in trivial cases (why?). Consider the case $n = 9 = 2^3 + 1$. In this case, every element in Z_9^* except 1 and -1 will result in the algorithm returning YES. Hence, the probability can be as bad as $(1 - \frac{2}{\phi(n)})$.