MTH6115 Cryptography Exercises 5 Solutions

Q1 (a) Instance: An $n \times n$ matrix $A = (a_{ij})$ with 0,1 entries. The size of this instance is n^2 since we can define A by specifying whether each entry is either zero or one. [10]

(b) The inverse matrix A^{-1}. [10]

(c) A non-zero linear combination of the rows (or columns) of A which is equal to the zero vector. [10]

(d) INVERTIBLE belongs to the complexity class P since we can use elementary row operations to reduce A to a matrix A^* in row echelon form. Then A is invertible if and only if A^* has no zero rows. [10]

Note. It is not obvious that the above answers can be accomplished in polynomial time. The certificate in (a) would not be polynomially verifiable if the number of bits needed to describe the entries in A^{-1} was not bounded by a fixed power of n. Similarly the certificate in (b) would not be polynomially verifiable if the number of bits needed to describe the coefficients in the linear combination was not bounded by a fixed power of n. GIVE 10 BONUS MARKS FOR ANY SENSIBLE COMMENTS ON THIS.

Q2 (a) The powers of 2 in $\mathbb{Z}_{41}$ are 2,4,8,16,32,23,5,10,20,40,..... Since $2^{10} \equiv 40 \equiv -1 \bmod 41$, we have $2^{20} \equiv (-1)^2 \equiv 1 \bmod 41$. Thus the order of 2 divides 20. Since $2^t \not\equiv 1 \bmod 41$ for all $1 \leq t \leq 10$, the order of 2 in $\mathbb{Z}_{41}$ must be 20. [10]

The powers of 3 in $\mathbb{Z}_{41}$ are 3,9,27,40,..... Since $3^4 \equiv 40 \equiv -1 \bmod 41$, we have $3^8 \equiv (-1)^2 \equiv 1 \bmod 41$. Thus the order of 3 divides 8. Since $3^t \not\equiv 1 \bmod 41$ for all $1 \leq t \leq 4$, the order of 2 must be 8. [10]

(b) We show that 6 is a primitive root modulo 41. We know that $6^{40} \equiv 1 \bmod 41$ by Fermat's Little Theorem. Hence the order of 6 divides 40. We have

$$6^{20} \equiv 2^{20}3^{20} \equiv 3^4 \equiv -1 \bmod 41$$

since 2 has order 20 and 3 has order 8. Similarly

$$6^{16} \equiv 2^{16}3^{16} \equiv (2^8)^2 \equiv 10^2 \equiv 18 \bmod 41$$

It follows that no proper divisor of 40 can be equal to the order of 6. Hence 6 is a primitive root modulo 41.

Q3 (a) We know that $x^{p-1} \equiv 1 \bmod p$ by Fermat's Little Theorem. Hence the order of x divides $p-1$. Since the order of x is a proper divisor of $p-1$ if and only if $x^t \equiv 1 \bmod p$ for some $1 \leq t \leq (p-1)/2$, we may decide if x is a primitive root by calculating $x^t \bmod p$ for all $1 \leq t \leq (p-1)/2$. [10]

(b) It is not a polynomial time algorithm since we have to calculate $(p-1)/2$ powers of x and the size of an instance of PRIMITIVE is $\log_2 x + \log_2 p$ [10]

Q4 Let $\phi(n) = q\lambda(n) + r$ where q, r are integers and $0 \leq r < \lambda(n)$. For each $x \in \mathbb{Z}_n$ with $\gcd(x, n) = 1$, we have $x^{\phi(n)} \equiv 1 \bmod n$ by Theorem 20 from lecture notes. Thus

$$1 \equiv x^{\phi(n)} \equiv x^{q\lambda(n)+r} \equiv x^{q\lambda(n)}x^r \equiv x^r \bmod n$$

since $x^{\lambda(n)} \equiv 1 \bmod n$. Since $r < \lambda(n)$, the definition of $\lambda(n)$ now implies that we must have $r = 0$. Thus $\phi(n) = q\lambda(n)$ and hence $\lambda(n)$ divides $\phi(n)$.

PLEASE GIVE FULL MARKS ALSO TO THE FOLLOWING PROOF (WHICH USES THE FACT THAT $\mathbb{Z}_n$ HAS AN ELEMENT OF ORDER $\lambda(n)$.)

Choose $x \in \mathbb{Z}_n$ such that x is coprime to n and such that the order of x is $\lambda(n)$. We know that $x^{\phi(n)} \equiv 1 \bmod n$ by Theorem 20 from lecture notes. The lemma we proved after Theorem 20, now implies that $\lambda(n)$ divides $\phi(n)$. [10]