MATH 195: CRYPTOGRAPHY
HOMEWORK #12

Problem 6.14. *Consider a Diffie-Hellman scheme with a common prime* $q = 11$ *and a primitive root* $\alpha = 2$.

(a) *If user A has public key* $Y_A = 9$, *what is A's private key* X_A*?*
(b) *If user B has public key* $Y_B = 3$, *what is the shared secret key* K*?*

Problem 7.17. *Given* 2 *as a primitive root of* 29, *construct a table of indices, and use it to solve the following congruences:*

(a) $17x^2 \equiv 10 \pmod{29}$;
(b) $x^2 - 4x - 16 \equiv 0 \pmod{29}$;
(c) $x^7 \equiv 17 \pmod{29}$.

Problem 6.25. *Prove that* $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$ *is a field of 9 elements, determine* $\mathrm{ord}(g)$ *for all* $g \in \mathbb{F}_9^*$, *and find a primitive root for* $\mathbb{F}_9$.

Problem 6.26. *Let* p *be a prime number for which* $2^p - 1$ *is prime (*$q = 2^p - 1$ *is called a* Mersenne prime*), and let* $f \in \mathbb{F}_2[X]$ *be irreducible of degree* p. *Let* $\mathbb{F}_{2^p}$ *be the field* $\mathbb{F}_2[X]/(f)$. *Prove:* X *is a primitive root for* $\mathbb{F}_{2^p}$, *i.e.* $\langle X \rangle = \mathbb{F}_{2^p}^*$.

Date: April 23, 2002.
6.14, 7.17, 6.25, 6.26.