CIS 3223 Homework 3

Dr Anthony Hughes

Name: Solutions
Temple ID (last 4 digits:

Simple non-graphing calculator

Make:

1 (16 pts) Answer the following.

(a) Find the smallest non-zero integer b such that $9b \equiv 0 \pmod{33}$

$\boxed{11}$

$\gcd(9, 33) = 3$

$b = \frac{33}{3} = 11$

$9 \times 11 = 99 \equiv 0 \pmod{33}$

(b) How many integers modulo 77 have inverses?

$\boxed{60}$

inverse $\Leftrightarrow$ unit

$\phi(77) = \varphi(7)\varphi(11) = 6 \times 10 = 60$

(c) Compute $2^{2024} \bmod 33$

$\boxed{16}$

$\varphi(33) = \varphi(3)\varphi(11) = 2 \times 10 = 20$

$2024 \equiv 4 \pmod{20}$

$2^{2024} \equiv_{33} 2^4 \equiv_{33} 16$

(d) 1.12(P39)

$\boxed{1}$

$\varphi(3) = 2$

2^{2006} even

$2^{2006} \equiv 0 \pmod{2}$

$2^{2^{2006}} \equiv_3 2^0 \equiv_3 1$

2 (15 pts) Use the **modular exponentiation** algorithm to calculate $3^{31} \pmod{37}$.

$z = 1$ $\quad 31_2 = 11111_2$

	digit	power	z
	1	3	3
1	1	9	$9 * 3 = 27$
3	1	$81 \equiv_{37} 7$	$7 * 27 = 189 \equiv_{37} 4$
7	1	$49 \equiv_{37} 12$	$12 * 4 = 48 \equiv_{37} 11$
15	1	$144 \equiv_{37} 33$	$33 * 11 = 363 \equiv_{37} 30$
31			

$\boxed{30}$

Consider an RSA key set with $p = 13$, $q = 17$, $N = 221$ and $e = 5$.

3 (12 pts) What value of d should be used for the secret key (show steps)? $\boxed{77}$

[Hint: Use the extended Euclidean algorithm]

$\varphi(221) = \varphi(13)\,\varphi(17) = 12 \times 16 = 192$

$\gcd(192, 5) = 1$

Solve $192x + 5y = 1$

a	b	q	r	Q
192	5	38	2	$\begin{bmatrix} 0 & 1 \\ 1 & -38 \end{bmatrix}$
5	2	2	1	$\begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & -38 \end{bmatrix} = \begin{bmatrix} 1 & -38 \\ -2 & 77 \end{bmatrix}$
2	1	2	0	$\begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 1 & -38 \\ -2 & 77 \end{bmatrix} = \begin{bmatrix} -2 & 77 \\ 5 & 192 \end{bmatrix}$

check

$y = 77$ (+ve)

$d = 77$

Could $e = 3$ be chosen? **yes** **no**

$\gcd(192, 3) = 3 \neq 1$

4 (7 pts). 1.19 (p 40)

Fact: $a = bq + r$. $\gcd(a, b) = \gcd(b, r)$ - Euclidean Algorithm

$F_{k+1} = F_k + F_{k-1} \Rightarrow \gcd(F_{k+1}, F_k) = \gcd(F_k, F_{k-1})$

So $\gcd(F_{n+1}, F_n) = \gcd(F_n, F_{n-1})$

$= \gcd(F_{n-1}, F_{n-2})$

$\vdots$

$\gcd(F_2, F_1) = 1$

Mathematically: Use induction

5 (extra credit, 4 pts) P42 Q38(a)

Want smallest n so that $10^n \equiv 1 \pmod{p}$, $n \mid \varphi(p)$

$p = 11$, $\varphi(11) = 10$, $n = 1, 2, 5, 10$ $\quad 10 \equiv_{11} 10$, $10^2 \equiv_{11} 1$ $\quad n = 2$

$p = 13$ $\quad \varphi(13) = 12$, $n = 1, 2, 3, 4, 6, 12$

$10^1 \equiv_{13} 10$, $10^2 \equiv_{13} 9$, $10^3 \equiv_{13} 12$, $10^4 \equiv_{13} 3$, $10^6 \equiv 1$ $\quad n = 6$

$p = 17$ $\quad \varphi(17) = 16$, $n = 1, 2, 4, 8, 16$

$10^1 \equiv_{17} 10$, $10^2 \equiv_{17} 15$, $10^4 \equiv_{17} 4$, $10^8 \equiv_{17} 16$, $10^{16} \equiv_{17} 1$ $\quad n = 16$

p=13 $\boxed{6}$ p=17 $\boxed{16}$