Problem set 6

(1) Use Hensel’s Lemma to solve $x^3 + x + 57 \equiv 0 \pmod{5^3}$.

(2) Use Corollary 4 from §II.F to solve $2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{7}$.

(3) Show that $3^8 \equiv -1 \pmod{17}$, and explain why this implies that $3$ is a primitive root mod $17$.

(4) Without finding them, how many solutions (if any) does $x^{20} \equiv 13 \pmod{17}$ have?

(5) Note that $2^3 \equiv 8 \pmod{23}$. By finding an inverse of $3$ in $\mathbb{Z}/22\mathbb{Z}$, find an integer $x$ such that $8^x \equiv 2 \pmod{23}$.

(6) Compute the following discrete logarithms: (a) $\log_{23} 13$ in $\mathbb{Z}/23\mathbb{Z}$, and (b) $\log_{10} 22$ in $\mathbb{Z}/47\mathbb{Z}$.

(7) Agnes and Bert use Diffie-Hellman key exchange to produce a shared secret key. They agree on $p = 101$ and an element $g = 15$ of order $p - 1$, both of which have been made public. Agnes chooses $\alpha$ and sends $g^\alpha = 42 \pmod{101}$ to Bert, while Bert has chosen $\beta$ and sent $g^\beta = 24$ to Agnes. As Ivan the interceptor, you overhear all this. By checking the first few powers of $g$ mod $101$, try to produce $\alpha$ or $\beta$ and hence their secret key $s$.

(8) Convert the decimal numbers 8734 and 5177 into binary numbers, combine them using XOR, then convert back to decimal. (You could think of 8734 as a message to be encrypted and 5177 as the key.)

(9) [for fun] Decrypt one of the messages in Hoffstein-Pipher-Silverman problem 1.4 (p. 48, a, b, or c – your choice).