Mathematics 243, section 1 – Algebraic Structures
Solutions for Practice Exam 2
November 3, 2003

I. A) Existence: Consider the set of integers $S = \{a - mb : m \in \mathbf{Z}\}$. S clearly contains positive integers. (If $a > 0$, then $a - mb > 0$ for all $m \leq 0$. If $a < 0$, we only need to take m sufficiently negative to get $a - mb > 0$). Hence the set $S^+ = S \cap \mathbf{Z}^+$ is nonempty. By the well-ordering principle, S^+ has a smallest element, call it $s = a - mb$. Note that $s \leq b$ since otherwise $s - b = a - (m+1)b > 0$ too, and s is not the smallest positive element of S. If $s = a - mb > 0$, then we can take $q = m$ and $r = s$ to get $a = qb + r$ satisfying the property that $0 \leq r < b$. On the other hand if $s = b$, then subtract one additional b from the equation $a - mb = s$ to get $a - (m+1)b = 0$, and take $q = m + 1, r = 0$. In either case we get q and r as claimed.

Uniqueness: We must show that if

$$a = q_1 b + r_1 \qquad a = q_2 b + r_2$$

with $0 \leq r_1, r_2 < b$, then $r_1 = r_2$ and $q_1 = q_2$. If we subtract the two equations for a, we get

$$0 = (q_1 - q_2)b + (r_1 - r_2). \tag{1}$$

Hence

$$(q_1 - q_2)b = (r_2 - r_1).$$

This says $r_2 - r_1$ is divisible by b. But $0 \leq r_1, r_2 < b$, so $0 \leq |r_2 - r_1| < b$. The only integer z with $0 \leq |z| < b$ that is divisible by b is $z = 0$. Hence $r_1 = r_2$, and we get $q_1 = q_2$ from (1).

B) $4578 = 19 \cdot 235 + 113$: $q = 19$, $r = 113$.

II. A) We say d is a greatest common divisor of a, b if
1) $d > 0$,
2) $d|a$ and $d|b$,
3) if $c|a$ and $c|b$, then $c|d$.

B) Using the Euclidean algorithm we have:

$$\begin{aligned} 488 &= 1 \cdot 376 + 112 \\ 376 &= 3 \cdot 112 + 40 \\ 112 &= 2 \cdot 40 + 32 \\ 40 &= 1 \cdot 32 + 8 \\ 32 &= 4 \cdot 8 + 0 \end{aligned}$$

so the last nonzero remainder gives the gcd: $\gcd(488, 376) = 8$. Then to find m, n with $m \cdot 488 + n \cdot 376 = 8$, set up our usual table:

k	r_k	q_k	m_k	n_k
-1	488		1	0
0	376		0	1
1	112	1	1	-1
2	40	3	-3	4
3	32	2	7	-9
4	8	1	-10	13

So $(-10)(488) + (13)(376) = 8$.

C) Suppose there is a solution x of the congruence $ax \equiv b \pmod{n}$. Then $n|(ax - b)$, so $ax - b = qn$ for some n, or

$$b = ax - qn. \tag{2}$$

Let $d = \gcd(a, n)$. Then $a = dq_1$ and $n = dq_2$. Substituting into the right side of (2), we get

$$b = (dq_1)x - q(dq_2) = d(q_1 x - qq_2).$$

Hence $d|b$.

III. The equation $[17][x] + [4] = [5]$ in $\mathbf{Z}_{29}$ will have just one solution. First add $-[4] = [25]$ to both sides, we get $[17][x] = [30] = [1]$. Since $\gcd(17, 29) = 1$, $[17]$ has a multiplicative inverse in $\mathbf{Z}_{29}$, $[17]^{-1} = [12]$ (see this by Euclidean algorithm again:

$$\begin{aligned} 29 &= 1 \cdot 17 + 12 \\ 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

so the last nonzero remainder gives the gcd: $\gcd(29, 17) = 1$.

k	r_k	q_k	m_k	n_k
-1	29		1	0
0	17		0	1
1	12	1	1	-1
2	5	1	-1	2
3	2	2	3	-5
4	1	2	-7	12

So $(-7)(29) + (12)(17) = 1$. So $[17]^{-1} = [12]$.) The solution of our equation is $[x] = [12][1] = [12]$.

IV. A) G corresponds to 6 and the RSA encryption function is $f([x]) = [x^e] = [x^19]$. We have by repeated squaring:

$$6^2 \equiv 36 \pmod{143}$$
$$6^4 \equiv 9 \pmod{143}$$
$$6^8 \equiv 81 \pmod{143}$$
$$6^{16} \equiv 126 \pmod{143}$$

Hence

$$6^{19} \equiv 6 \cdot 6^2 \cdot 6^{16} \pmod{143} \equiv 46 \pmod{143}$$

and G encrypts to 46.

B) First we factor $m = 143 = 11 \cdot 13$, so $p = 11$, and $q = 13$ are the two primes. The decryption exponent d satisfies

$$de \equiv 1 \pmod{(p-1)(q-1) = 120}$$

$d = 19$ is the solution of this (it's the multiplicative inverse of $[19]$ in $\mathbf{Z}_{120}$ (find using Euclidean algorithm as above). Hence $102^{19} \equiv 15 \pmod{143}$, which corresponds to a P.