UNIVERSITY OF MANITOBA
TEST 1 SOLUTIONS

COURSE: MATH 2170 DURATION: 45 minutes
DATE & TIME: February 11, 2019, 16:30–17:15

I understand that cheating is a serious offence:

Signature: _____
(*In Ink*)

---

1. Let a, b, m, be integers, $m > 1$.

[1] (a) Define $a|b$.

> **Solution:** $a|b$ iff for some d, $ad = b$.

[1] (b) Define $a \equiv b \pmod{m}$.

> **Solution:** $a \equiv b \pmod{m}$ iff $m|(b-a)$.

[4] (c) Complete each of the following equations (no explanation required):

i. $(a, 0) =$ _____
ii. $(a, 1) =$ _____
iii. $[a, 0] =$ _____
iv. $[a, 1] =$ _____

> **Solution:**
>
> i. $(a, 0) = a$
>
> ii. $(a, 1) = 1$
>
> iii. $[a, 0] = 0$
>
> iv. $[a, 1] = a$

2. Let a, b, m, be integers, $m > 1$.

[3] (a) Prove that if $(a, m) = 1$ and $(b, m) = 1$ then $(ab, m) = 1$.

Note: Prove this using properties of the gcd and of divisibility, *not* properties of prime numbers.

Solution: There are x and y such that $ax + my = 1$, and there are u and v so that $bu + mv = 1$.

So $ax = 1 - my$ and $bu = 1 - mv$.

Therefore $ab(xu) = (1 - my)(1 - mv) = 1 - m(x + y - mxy)$, so $(ab, m) = 1$.

Solution: Note: A solution by checking common prime divisors, contrary to the instructions, was worth at most 1. [This result was one of the tools that we used to *prove* the properties of prime numbers.]

Suppose $1 < d = (ab, m)$. Then there is a prime p, $p|d$. Thus $p|ab$ and $p|m$. Since p is prime, $p|a$ or $p|b$ (and $p|m$). But $(a, m) = 1$ and $(b, m) = 1$,, a contradiction.

[3] (b) Prove that if $c|ab$ and $(b, c) = 1$, then $c|a$.

Solution: $(ab, ac) = a(b, c) = a$.

But $c|ab$ and $c|ac$, so $c|a$.

Solution: Since $(b, c) = 1$ there are integers x and y such that $bx + cy = 1$. Thus $abx + acy = a$. By assumption $c|ab$, and certainly $c|ac$. Therefore $c|a$.

---

[8] 3. Using the Euclidean algorithm, **and the specific algorithm taught in class and in the textbook**, determine $d = (10680, 4628)$ and two integers x and y so that $d = 10680x + 4628y$.

Solution: We learned the following formulas: $r_{-1} = a$, $r_0 = b$, q_{i+1} is determined by division: $r_{i-1} = r_i q_{i+1} + r_{i+1}$, $0 \leq r_{i+1} < r_i$, so we get rules as follows (with $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$, and $y_0 = 1$):

$$\begin{cases} r_k &= r_{k-2} - q_k r_{k-1} \\ x_k &= x_{k-2} - q_k x_{k-1} \\ y_k &= y_{k-2} - q_k y_{k-1} \end{cases}$$

Therefore in this case:

q_{i+1}	r_i	x_i	y_i
	10680	1	0
2	4628	0	1
3	1424	1	−2
4	356	−3	7
	0		

Therefore $d = 356 = -3 \times 10680 + 7 \times 4628$.

Note: A "long form" solution contrary to the instructions is worth a maximum of 4 points.

[2] 4. (a) Define "p is a prime number".

> **Solution:** An integer p is a *prime number* if $p > 1$ and there is no divisor d of p with $1 < d < p$.
>
> or
>
> An integer $p > 1$ is a *prime number* if p has exactly two positive divisors, namely itself and 1.

Note: It is an *essential* part of this definition that p be greater than 1, and that reference is made to *positive* divisors. Otherwise, we would have to consider 1 and -1 to be primes, and we would have to contend with the *four* divisors of p: 1, -1, p, $-p$.

[4] (b) Prove that there are infinitely many prime numbers.

> **Solution:** Suppose that $p_1, \ldots, p_n$ is a list of all the prime numbers.
> Let $N = p_1 \times \cdots \times p_n + 1$.
> N has a prime divisor p.
> The remainder on dividing N by any one of $p_1, \ldots, p_n$ is 1, so p is not one of $p_1, \ldots, p_n$.
> Therefore $p_1, \ldots, p_n$ was *not* a list of all the prime numbers.
>
> Alternatively, suppose P is the largest prime number and let $N = P! + 1$.
>
> **Note**: It is not enough to say that N is not divisible by any of the p_i; you need to say why.

---

[2] 5. (a) Define Euler's function $\phi(m)$.

> **Solution:** $\phi(m)$ is the number of elements in a reduced residue system modulo m.
>
> or
>
> $\phi(m)$ is the number of positive integers less than or equal to m and relatively prime to m,.

[2] (b) State Euler's Theorem.

> **Solution:** If $(a,\, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

[2] (c) Give a reduced residue system modulo 10 consisting of multiples of 3.

> **Solution:** The usual reduced residue system modulo 10 is 1, 3, 7, 9. Adding multiples of 10 to any item in the list does not change the fact that this is a reduced residue systemt modulo 10.
>
> So we get 21, 3, 27, 9 as one possible answer amongst many.

---

[4] 6. Find the least positive residue of 50! modulo 53 .

Solution: By Wilson's Theorem, $52! \equiv -1 \pmod{53}$ since 53 is a prime. So:

$-1 \equiv 52! \equiv 50!(51)(52) \equiv 50!(-2)(-1) \equiv 50!(2) \pmod{53}$.

But clearly $2 \times 27 = 54 \equiv 1 \pmod{53}$, so:

$(-1)27 \equiv 50!(2)(27) \equiv 50! \pmod{53}$.

Therefore

$$50! \equiv -27 \equiv 26 \pmod{53}$$