MATH 3H03 (NUMBER THEORY)
DUE: FEBRUARY 28, 2020

HOMEWORK ASSIGNMENT 5

All of the questions from Part A will be graded. For Part B, do questions 4 and 5 (one of which will be graded completely and the other for completion) **or** do question 6. Assignments will be submitted via *Crowdmark*.

Part A. [Short Questions; 6pts]

Exercise 1. Solve the linear congruence $140x \equiv 133 \pmod{301}$.

Exercise 2. Consider the polynomial

$$f(x) = 16x^{11} + 13x^9 + 10x^7 + 7x^5 + 4x^3 + x.$$

Find a polynomial $g(x)$ with $\deg g(x) \leq 7$ and $f(x) \equiv g(x) \pmod 7$ for all integers x.

Exercise 3. Show that 645 is a pseudo-prime. [HINT: It is clear that $645 = 5 \cdot 129$ is not prime. Reduce the question to proving $2^{645} \equiv 2 \pmod 5$ and $2^{645} \equiv 2 \pmod{129}$.]

Part B. [Proof Questions; 6pts]

Exercise 4. (The following problem is due to Regiomontanus 1436-1476.) Find an integer having the remainders $3, 11, 15$ when divided by $10, 13, 17$ respectively.

Exercise 5. Let $n = 2p$ with p an odd prime. Show that $a^{n-1} \equiv a \pmod n$ for all integers a.

Exercise 6. (For students who have taken Math 3GR3.) Let R be a commutative ring with identity 1_R, and let I and J be ideals of R. Suppose also that $I + J = \langle 1_R \rangle$. Consider the map

$$\phi : R \to R/I \times R/J$$

defined by $a \mapsto (a + I, a + J)$. Show that

(a) The map ϕ is a ring homomorphism.
(b) The homomorphism ϕ is surjective. (Try to adapt the proof of Theorem 3.10.)
(c) Show the kernel of ϕ is $\ker(\phi) = I \cap J$.
(d) Use the above results to show that if $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

REMARK: Note that by part (d), for any $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, there is exactly one $c \in \mathbb{Z}_{mn}$ that is associated to (a, b). The Chinese Remainder Theorem can be viewed as the procedure by which one can find this c.