College of the Holy Cross, Fall Semester 2017
MATH 243 – Mathematical Structures, section 2
Solutions for Exam 3 – December 7

I. (25) Give the statement and proof of "Fermat's Little Theorem."

Solution: The statement is that if p is prime in $\mathbb{Z}$ and $\gcd(a,p) = 1$. Then $a^{p-1} \equiv 1 \bmod p$.

Proof: Since $\gcd(a,p) = 1$, the class $[a] \in \mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. We claim this implies that the mapping $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $f([x]) = [a][x]$ is injective and surjective. Injectivivity follows because if $f([x]) = [a][x] = [a][x'] = f([x'])$, then we can multiply both sides of this equation by $[a]^{-1}$ to obtain $[x] = [x']$. This shows that f is injective. Then, since $\mathbb{Z}/p\mathbb{Z}$ is finite, f must be surjective as well. Now $f([0]) = [0]$. Hence f must map the nonzero classes in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ to themselves it follows that the $[a], [2a], \ldots, [(p-1)a]$ are the same as $[1], [2], \ldots, [p-1]$, just in a different order. But then it follows that

$$\begin{aligned}(p-1)! \bmod p &= (p-1) \cdot (p-2) \cdots 2 \cdot 1 \bmod p \\ &\equiv (p-1)a \cdot (p-2)a \cdot \cdots 2a \cdot a \bmod p \\ &= a^{p-1} \cdot (p-1)! \bmod p.\end{aligned}$$

Since all of the factors b in $(p-1)!$ satisfy $\gcd(b,p) = 1$, $(p-1)!$ also has a multiplicative inverse mod p, so this congruence implies

$$1 \equiv a^{p-1} \bmod p,$$

which is what we wanted to show.

II. (20) An RSA public key encryption system has public key $m = 551, e = 11$. "Crack the code" by determining the private key information: p, q, d.

Solution: We see $m = 551 = 19 \cdot 29$, and both factors are prime, so $p = 19$ and $q = 29$ (or vice versa – either is OK). Then recall that the decryption exponent must satisfy

$$e \cdot d \equiv 1 \bmod (p-1)(q-1),$$

So we need to determine a multiplicative inverse of $e = 11 \bmod (p-1)(q-1) = 18 \cdot 28 = 504$. We do this by the Euclidean algorithm:

$$\begin{aligned}504 &= 45 \cdot 11 + 9 \\ 11 &= 1 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1.\end{aligned}$$

So applying the Extended Euclidean Algorithm

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 45 & 1 & -45 \\ 1 & -1 & 46 \\ 4 & 5 & -229 \end{array}$$

So the multiplicative inverse is $-229 \equiv 275 \bmod 504$. We would use the decryption exponent $d = 275$ to decrypt intercepted messages.

III. Let $f : A \to B$ be a mapping.

(A) (10) Show that if U_1, U_2 are subsets of B, then $f^{-1}(U_1 \cap U_2) = f^{-1}(U_1) \cap f^{-1}(U_2)$.

Solution: $\subseteq$: Let $x \in f^{-1}(U_1 \cap U_2)$. Then $f(x) \in U_1 \cap U_2$, so $f(x) \in U_1$ and $f(x) \in U_2$. By definition this means that $x \in f^{-1}(U_1)$ and $x \in f^{-1}(U_2)$. Hence $x \in f^{-1}(U_1) \cap f^{-1}(U_2)$. This shows the $\subseteq$ inclusion.

$\supseteq$: Now assume $x \in f^{-1}(U_1) \cap f^{-1}(U_2)$. This implies $x \in f^{-1}(U_1)$ and $x \in f^{-1}(U_2)$, so by definition, $f(x) \in U_1$ and $f(x) \in U_2$. But that shows $f(x) \in U_1 \cap U_2$, so $x \in f^{-1}(U_1 \cap U_2)$. Hence we get the $\supseteq$ inclusion as well.

(B) (10) If f is injective, and T_1, T_2 are subsets of A, show that $f(T_1) \cap f(T_2) \neq \emptyset$ implies $T_1 \cap T_2 \neq \emptyset$.

Solution: If $y \in f(T_1) \cap f(T_2)$, then $y = f(x_1)$ for some $x_1 \in T_1$ and $y = f(x_2)$ for some $x_2 \in T_2$. But that implies $f(x_1) = f(x_2)$ and f is assumed injective, so $x_1 = x_2$. This shows $x_1 = x_2 \in T_1 \cap T_2$, so $T_1 \cap T_2 \neq \emptyset$.

IV. (15) Let R be the relation on $\mathbb{R}\backslash\{0\}$ defined by $a \; R \; b \Leftrightarrow \frac{a}{b} \in \mathbb{Q}$. See below.[1] Is R an equivalence relation? Prove your assertion.

Solution: Yes this is an equivalence relation:

(1) R is reflexive since $\frac{a}{a} = 1 \in \mathbb{Q}$ for all $a \in \mathbb{R} \setminus \{0\}$. So $a \; R \; a$ is true for all $a \neq 0$.

(2) R is symmetric since $a \; R \; b$ says $\frac{a}{b} = \frac{m}{n} \in \mathbb{Q}$ implies $\frac{b}{a} = \frac{n}{m} \in \mathbb{Q}$ (note $m \neq 0$ follows because $a, b \neq 0$). Hence $a \; R \; b$ implies $b \; R \; a$.

(3) R is transitive since if $a \; R \; b$ and $b \; R \; c$, then $\frac{a}{b} = \frac{m}{n}$ and $\frac{b}{c} = \frac{p}{q}$ with m, n, p, q in $\mathbb{Z}$. But then

$$\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c} = \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$$

so $a \; R \; c$ as well.

[1]Here $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}$ is the set of rational numbers.

V.

(A) (10) Show that $\mathbb{N}$ is not bounded above in the real numbers.

Solution: (by contradiction): Assume that $\mathbb{N}$ is bounded above. Then Axiom C for the real number system implies that $\mathbb{N}$ has a least upper bound, call it b. But then by definition of a least upper bound, if we consider $b-1<b$, there must be a natural number $n \in \mathbb{N}$ with $b-1<n \leq b$. But that implies $(b-1)+1=b<n+1$, and $n+1 \in \mathbb{N}$, but $n+1>b$. Hence b cannot be an upper bound for $\mathbb{N}$. This contradiction shows $\mathbb{N}$ has no upper bound in $\mathbb{R}$.

(B) (10) Use part (A) to show that for all real numbers $\varepsilon>0$, there exist $n \in \mathbb{N}$ such that $\left|1-(1+\frac{(-1)^n}{\sqrt{n}})\right|<\varepsilon$

Solution: If we simplify we get

$$\left|1-\left(1+\frac{(-1)^n}{\sqrt{n}}\right)\right|=\frac{1}{\sqrt{n}}$$

We will have

$$\frac{1}{\sqrt{n}}<\varepsilon \Leftarrow n>\frac{1}{\varepsilon^2}$$

Since $\mathbb{N}$ is not bounded in $\mathbb{R}$, no matter how small ε is, and consequently, no matter how big $\frac{1}{\varepsilon^2}$ is, there are still $n>\frac{1}{\varepsilon^2}$. This is equivalent to $\frac{1}{\sqrt{n}}<\varepsilon$.