

Math 52B Solutions to Practice Problems

1. a. $S \subseteq S \Rightarrow S \subseteq T$
b. $a \in S \Rightarrow a \equiv 3 \pmod{5}$ by def. of S
 $\Rightarrow a^2 \equiv 3^2 \pmod{5}$ by rules of modular arithmetic
 $\Rightarrow a^2 \equiv 4 \pmod{5}$ since $3^2 = 9 \equiv 4 \pmod{5}$ and congruence is transitive
 $\Rightarrow a \in T$ by def. of T .

We have shown by combining these steps that $a \in S \Rightarrow a \in T$ and therefore $S \subseteq T$.

- c. $S \subseteq S$ for any set S so $(S, S) \in \rho$ and ρ is reflexive
If $S \subseteq T$ and $T \subseteq S$ then $S = T$, by def. of equality of sets. So $(S, T) \in \rho$ and $(T, S) \in \rho \Rightarrow S = T$.
This shows that ρ is antisymmetric.

If $S \subseteq T$ and $T \subseteq W$ then $S \subseteq W$ because $s \in S \Rightarrow s \in T$ and $s \in T \Rightarrow s \in W$ so $s \in S \Rightarrow s \in W$.

Thus $(S, T) \in \rho$ and $(T, W) \in \rho \Rightarrow (S, W) \in \rho$.

This shows that ρ is transitive. Since ρ is reflexive, ^{anti-}symmetric and transitive, ρ satisfies the definition of a partial order.

- d. $T_1 \sim T_1$ because we can choose $r = 1$.

So the relation is reflexive

If $T_1 \sim T_2$ by multiplication by r , we see that $T_2 \sim T_1$ by multiplication by $1/r$. So symmetric.

If $T_1 \sim T_2$ by multiplication by r_1 and $T_2 \sim T_3$ by multi by r_2 , we see that

$T_1 \sim T_3$ by mult by $r_2 r_1$, so transitive.

Since the relation is reflexive, symmetric and transitive, it is an equivalence relation.

1 e. Let T_0 be the equilateral triangle whose sides have length 1. If T is any equilateral triangle, let l be the length of its sides. Then $T_0 \sim T$ by mult. by $r=l$. So T is equivalent to T_0 , which means that T is in the equivalence class of T_0 . This is true for any equilateral triangle T , so they are all in the equivalence class of T_0 .

1 f. Let T_n be the isosceles triangle whose sides have length 1, 1 and $\frac{1}{n}$, for $n \in \mathbb{Z}^+$. Then an equivalent triangle would have sides of length $r, r, \frac{r}{n}$. If this is T_m with sides 1, 1 and $\frac{1}{m}$, we can see that $r=1$ and $n=m$. So if $1 < n < m \in \mathbb{Z}^+$, $T_n \not\sim T_m$. So T_n and T_m are in different equiv. classes. This means that the equivalence classes $[T_2], [T_3], [T_4], \dots$ are all different, and there are infinitely many.

2. $P(n): a^n \equiv b^n \pmod m$, to be proved by induction on n .

Basis step: $a^1 \equiv b^1 \pmod m$ is true because we are given that $a \equiv b \pmod m$. This proves $P(1)$.

Inductive step: We assume $P(N)$, the inductive hypothesis, so $a^N \equiv b^N \pmod m$. Also $a \equiv b \pmod m$ because this was given. We use the rule of modular arithmetic for multiplication.

It says that if $a_1 \equiv b_1 \pmod m$ and $a_2 \equiv b_2 \pmod m$ then $a_1 a_2 \equiv b_1 b_2 \pmod m$. Take $a_1 = a, b_1 = b, a_2 = a^N, b_2 = b^N$. The rule applies, and we get

$a^N \equiv b^N \pmod{m}$. Using rules for exponents, this may be written as $a^{N+1} \equiv b^{N+1} \pmod{m}$. Hence $P(N+1)$ is true. We have completed the inductive step and can conclude that $P(n)$ is true for all pos. integers n . In other words, $a^n \equiv b^n \pmod{m}$ for all $n \in \mathbb{Z}^+$.

3a. The extended Euclidean algorithm begins with $a, b \in \mathbb{Z}^+$. First one applies the division algorithm to get $a = bq + r_1$, with $0 \leq r_1 < b$. Then a and b are replaced by b and r_1 . One repeats this until reaching $r_k = 0$. Then $\gcd(a, b) = r_{k-1}$. Furthermore one can substitute back to get $\gcd(a, b) = ax + by$, for some $x, y \in \mathbb{Z}$.

b. The extended Euclidean algorithm gives $ax + by = g$. Now if $d|a$ and $d|b$, this means $a = da_1$ and $b = db_1$, with $a_1, b_1 \in \mathbb{Z}$. Substituting in, we have $g = ax + by = da_1x + db_1y = d(a_1x + b_1y)$. So $g = d(a_1x + b_1y)$, which shows that $d|g$, since $a_1x + b_1y \in \mathbb{Z}$.

c. First we find $37^{-1} \pmod{423}$.

$$(423) = (37)11 + (16)$$

$$(37) = (16)2 + (5)$$

$$(16) = (5)3 + (1) \quad \text{so } (1) = (16) - 3(5) = (16) - 3[(37) - 2(16)]$$

$$= 7(16) - 3(37)$$

$$= 7[423 - 11(37)] - 3(37) = 7(423) - 80(37)$$

$$1 = 7(423) - 80(37) \quad \text{so } 1 \equiv -80(37) \pmod{423}$$

$$\text{This shows } -80 \equiv 37^{-1} \pmod{423}.$$

Now to solve $37x \equiv 51 \pmod{423}$ for x ,
we multiply both sides by -80 and get

$$x = 1 \cdot x \equiv -80 \cdot 37x \equiv -80 \cdot 51 \pmod{423}.$$

$$\text{So } x \equiv -4080 \pmod{423} \Rightarrow x \equiv -273 \equiv \boxed{150 \pmod{423}}$$

We can check this answer by multiplying.

4. a. $x = x_1 b + d_0$ by div. alg.

$$x_1 = x_2 b + d_1 \quad \text{"}$$

$$x_2 = x_3 b + d_2 \quad \text{"}$$

etc.

$$x = (\dots d_2 d_1 d_0)_b.$$

b. Yes it solves a type of problem correctly in a finite number of prescribed steps.

$$\left. \begin{array}{l} 213 = 42 \cdot 5 + 3 \\ 42 = 8 \cdot 5 + 2 \\ 8 = 1 \cdot 5 + 3 \\ 1 = 0 \cdot 5 + 1 \end{array} \right\} 213 = (1323)_5$$

$$d. (0.314)_5 = \frac{3}{5} + \frac{1}{25} + \frac{4}{125} = \frac{3 \cdot 25 + 1 \cdot 5 + 4}{125} = \frac{84}{125} \text{ or } .672$$

$$\begin{aligned} e. & (a_1 a_2 a_1 a_2 a_1 a_2 \dots)_b \\ &= \left(\frac{a_1}{b} + \frac{a_2}{b^2} \right) + \left(\frac{a_1}{b^3} + \frac{a_2}{b^4} \right) + \left(\frac{a_1}{b^5} + \frac{a_2}{b^6} \right) + \dots \\ &= \left(\frac{a_1}{b} + \frac{a_2}{b^2} \right) \left(1 + \frac{1}{b^2} + \frac{1}{b^4} + \dots \right) \\ & \quad \text{(geometric series)} \\ &= \left(\frac{a_1 b + a_2}{b^2} \right) \left(\frac{1}{1 - 1/b^2} \right) = \frac{a_1 b + a_2}{b^2 - 1} \end{aligned}$$

5. a. Two logical statements are equivalent if they have the same truth table.

b.

A	B	$A \vee B$	$A \wedge (A \vee B)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

Using the def. of \vee and \wedge , we constructed the table. The last column is the same as the first. So A is equiv. to $A \wedge (A \vee B)$

c. Converse: If you know modular arithmetic, then you ace Math 52.

Contrapositive: If you don't know modular arithmetic, then you don't ace Math 52.

The contrapositive is equivalent to the original (which is presumably true, on the other hand, the converse is presumably not true. You may know modular arithmetic, but not relations, functions, and induction. This would prevent you from acing Math 52.

6. a) A function is a relation f from S to T whose domain is S and such that every $s \in S$ is related to at most one $t \in T$. (If $s \in S$, there is one and only one $t \in T$ such that $(s, t) \in f$)

b) $2 \in S$ is paired with only $8 \in T$
 $4 \in S$ is paired with only $7 \in T$
 $6 \in S$ is paired with only $9 \in T$

c) A function f is 1-1 if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

d) $8 \in T$ is paired only with $2 \in S$, $7 \in T$ only with $4 \in S$, $9 \in T$ with $6 \in S$

$7 \in T$ is not paired with any elt. of S .

So each element of T is paired with at most one elt. of S . This shows σ is 1-1.

e. σ has no inverse because σ is not onto, and a function has an inverse if and only if it is 1-1 and onto. In particular, $7 \in T$, but there is no s with $\sigma(s) = 7$.

f. $\sigma^{-1} = \{(8, 2), (7, 4), (9, 6)\}$ as a function from R to S .

g. $f \circ g(a_1) = f \circ g(a_2) \Rightarrow f(g(a_1)) = f(g(a_2))$
by def. of composition

$\Rightarrow g(a_1) = g(a_2)$ since f is 1-1

$\Rightarrow a_1 = a_2$ since g is 1-1.

Thus $f \circ g(a_1) = f \circ g(a_2) \Rightarrow a_1 = a_2$.

This shows that $f \circ g$ is 1-1, by def.

h. Since f^{-1} is the inverse of f , this means that

$f^{-1}(f(x)) = x$, for all x . To show that

$g^{-1} \circ f^{-1}$ is the inverse of $f \circ g$, we need to show that $(g^{-1} \circ f^{-1})(f \circ g(y)) = y$ for all y ,

and $(f \circ g)(g^{-1} \circ f^{-1}(z)) = z$ for all z .

This is easy to check using the above with $x = g(y)$:

$$(g^{-1} \circ f^{-1})(f \circ g(y)) = (g^{-1} \circ f^{-1})(f(g(y)))$$

$$= g^{-1}(f^{-1}(f(g(y)))) = g^{-1}(g(y)) = y.$$

$$\text{Also } (f \circ g)(g^{-1} \circ f^{-1}(z)) = f(g(g^{-1}(f^{-1}(z)))) = f(f^{-1}(z)) = z$$

7 a)

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

b) The only factors of p are 1 and p , since it is prime. Since p is not a factor of 2, since $p > 2$, the only common factor of 2 and p is 1, so $\gcd(2, p) = 1$. We know that this implies that 2 has an inverse mod p .

c) Since $b = 2^{-1} \pmod{p}$, we get $2b \equiv 1 \pmod{p}$.

Then $g(f(x)) \equiv g(2x) \equiv b \cdot 2x \equiv x \pmod{p}$.

Since $x \in \mathbb{Z}/p\mathbb{Z}$, and $g(f(x)) \in \mathbb{Z}/p\mathbb{Z}$, this

means $g(f(x)) = x$. Similarly $f(g(y)) = y$.

So g is the inverse function of f .

d) Since f has an inverse, namely g , as shown in part c), f is a bijection (1-1 and onto)

e) Since f is a bijection from $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ to itself, the numbers $\{0, 1, 2, \dots, p-1\}$

are the same set of numbers as $\{f(0), f(1), f(2), \dots, f(p-1)\}$

Leaving out $0 = f(0)$, we have

$$\{1, 2, \dots, p-1\} = \{2 \cdot 1 \pmod{p}, 2 \cdot 2 \pmod{p}, 2 \cdot 3 \pmod{p}, \dots, 2 \cdot (p-1) \pmod{p}\}$$

Since we have the same set of numbers in a

different order, the product will be the same!

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) = (2 \cdot 1 \pmod{p})(2 \cdot 2 \pmod{p}) \cdot \dots \cdot (2 \cdot (p-1) \pmod{p})$$

Simplifying and using $(a \bmod p)(b \bmod p) \equiv ab \pmod p$
 we get $(p-1)! \equiv 2^{p-1} (p-1)! \pmod p$ (See Thm 3.12 in the text for a more general pf.)

f. Again $(p-1)!$ has no factors in common with p ,
 so it has an inverse (all its factors are $< p$).
 Multiplying by this inverse mod p gives.

$$1 \equiv 2^{p-1} \pmod p.$$

g. $\phi(m)$ is the number of integers in $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \dots, m-1\}$
 that are relatively prime to m .

h. $A \equiv a \pmod{mn} \Rightarrow A = a + kmn \Rightarrow A = a + k_1 n, k_1 = km$
 $\Rightarrow A = a + k_2 m, k_2 = kn$
 $\Rightarrow A \equiv a \pmod n$ and $A \equiv a \pmod m$.

For a counterexample to the converse, we can take
 $A = 5, a = 1, m = 2, n = 4$. That is

$$5 \equiv 1 \pmod 2 \text{ and } 5 \equiv 1 \pmod 4, \text{ but } 5 \not\equiv 1 \pmod{8 = 2 \cdot 4}.$$

If $\text{GCD}(m, n) = 1$, and $A \equiv a \pmod m, A \equiv a \pmod n$,
 the Chinese remainder thm says that since
 $A \pmod{mn}$ and $a \pmod{mn}$ are both congruent to
 $a \pmod m$ and $a \pmod n$ and in $\mathbb{Z}/mn\mathbb{Z}$,
 they must be equal. This means $A \equiv a \pmod{mn}$.

i. By Fermat's Little Thm, $a^{12} \equiv 1 \pmod{13}$ and
 $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$. Thus

$$a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod 7 \text{ and}$$

$$a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod 5$$

So $a^{12} \equiv 1 \pmod{13}$ and $a^{12} \equiv 1 \pmod{7}$.

By part h, we can conclude that $a^{12} \equiv 1 \pmod{13 \cdot 7}$,
since $\gcd(13, 7) = 1$.

By part h again, we can conclude that since

$a^{12} \equiv 1 \pmod{5}$ also, we have $a^{12} \equiv 1 \pmod{13 \cdot 7 \cdot 5}$
because $\gcd(13 \cdot 7, 5) = 1$.

8. a) $(\cos(\theta) + i \sin(\theta))^n = \cos(n\theta) + i \sin(n\theta)$ or $(e^{i\theta})^n = e^{in\theta}$

b) Let $z = a + bi$, so $\bar{z} = a - bi$

$$\begin{aligned} \text{Then } e^{\bar{z}} &= e^{a-bi} = e^a e^{-bi} = e^a (\cos(b) - i \sin(b)) \\ &= e^a (\cos(b) - i \sin(b)) = e^a \overline{(\cos(b) + i \sin(b))} \\ &= e^a \overline{e^{bi}} = e^a \cdot e^{-bi} = \overline{e^{a+bi}} = \overline{e^z} \end{aligned}$$

since \sin is odd, \cos is even, and the conjugate of a product is the product of the conjugates.

c) $(e^{i\theta})^{-1} = \frac{1}{e^{i\theta}} = \frac{1}{e^{i\theta}} \cdot \frac{\overline{e^{i\theta}}}{\overline{e^{i\theta}}} = \frac{\overline{e^{i\theta}}}{e^{i\theta} \overline{e^{i\theta}}} = \frac{e^{-i\theta}}{e^{i\theta} e^{i\theta}}$ by part b).

$$\begin{aligned} &= \frac{e^{-i\theta}}{e^{i\theta} e^{i\theta}} = \frac{e^{-i\theta}}{e^{i\theta} e^{i(-\theta)}} = \frac{e^{-i\theta}}{e^{i(\theta-\theta)}} \quad \text{by multiplic. in polar form} \\ &= \frac{e^{-i\theta}}{e^0} = \frac{e^{-i\theta}}{1} = e^{-i\theta} \end{aligned}$$

d) $(e^{i\theta})^{-m} = \frac{1}{(e^{i\theta})^m} = \frac{1}{e^{im\theta}}$ by De Moivre
 $= (e^{im\theta})^{-1} = e^{-im\theta}$ by part c).

e) $\frac{2-7i}{3+4i} \cdot \frac{3-4i}{3-4i} = \frac{6-21i-8i+28i^2}{9+16} = \frac{-22-29i}{25} = -\frac{22}{25} - \frac{29}{25}i$