CS 173: Discrete Structures, Summer 2014
Homework 2

This homework contains 5 problems, each worth 10 points. It is due in class on Wednesday, July 2nd. **Please follow the guidelines on the class web page about homework format and style.**

In all questions, you must explain how you get your answers. Stating the answer with no supporting work will not receive full credit.

1. **Prime modulus**

   (a) Prove that if x is an integer, p is a prime, and $x^2 \equiv 1 \pmod{p}$, then either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$ or both. (Hint: Use Euclid's lemma.)

   Solution. Suppose $x \in \mathbb{Z}$ and p is prime. Then,

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\implies p \mid x^2 - 1 && (1)\\ &\implies p \mid (x+1)(x-1). && (2) \end{aligned}$$

   By Euclid's lemma, either $p \mid (x+1)$ or $p \mid (x-1)$.
   Case 1: $p \mid (x+1)$. In this case,

$$x + 1 \equiv 0 \pmod{p} \implies x \equiv -1 \pmod{p}.$$

   Case 2: $p \mid (x-1)$. In this case,

$$x - 1 \equiv 0 \pmod{p} \implies x \equiv 1 \pmod{p}.$$

   In both cases, either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$, as desired. $\square$

   (b) Show that this statement is false if p is allowed to be composite. (In other words, disprove the following statement: If x and p are integers, p is positive, and $x^2 \equiv 1 \pmod{p}$, then either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$ or both.)

   Solution. The statement we want to disprove is

$$\forall x \in \mathbb{Z}, \forall p \in \mathbb{Z}^+, [x^2 \equiv 1 \pmod{p}] \to [x \equiv 1 \pmod{p} \vee x \equiv -1 \pmod{p}]$$

   The negation of this is:

$$\exists x \in \mathbb{Z}, \exists p \in \mathbb{Z}^+, x^2 \equiv 1 \pmod{p} \wedge x \not\equiv 1 \pmod{p} \wedge x \not\equiv -1 \pmod{p}.$$

   To prove this negation, let $x = 3$ and $p = 8$. Then,

$$\begin{aligned} 3^2 &\equiv 1 \pmod{8}, && (3)\\ 3 &\not\equiv 1 \mod 8, && (4)\\ 3 &\not\equiv -1 \mod 8, && (5) \end{aligned}$$

   as desired. $\square$

2. **Extended Euclidean algorithm**

(a) Let $a = 826$ and $b = 470$. Find a pair of integers (s_1, t_1) such that $s_1 a + t_1 b = \gcd(a, b)$.

Solution. Running Euclid's algorithm, we get

$$\begin{aligned} 826 &= 1(470) + 356 && (6)\\ 470 &= 1(356) + 114 && (7)\\ 356 &= 3(114) + 14 && (8)\\ 114 &= 8(14) + 2 && (9)\\ 14 &= 7(2). && (10) \end{aligned}$$

Thus, $\gcd(a, b) = 2$ and

$$\begin{aligned} 2 &= 114 - 8(14) && (11)\\ &= (470 - 356) - 8(356 - 3(114)) && (12)\\ &= 470 - 9(356) + 24(114) && (13)\\ &= 470 - 9(826 - 470) + 24(470 - 356) && (14)\\ &= 34(470) - 9(826) - 24(356) && (15)\\ &= 34(470) - 9(826) - 24(826 - 470) && (16)\\ &= 58(470) - 33(826), && (17) \end{aligned}$$

so $(s_1, t_1) = \boxed{(-33, 58)}$ works. □

(b) Find a different pair of integers (s_2, t_2) such that $s_2 a + t_2 b = \gcd(a, b)$. (Hint: Find integers s and t such that $sa + tb = 0$. What is $(s_1 + s)a + (t_1 + t)b$?)

Solution. We have

$$\begin{aligned} &(470 - 33)826 + (58 - 826)470 && (18)\\ &= [(-33)826 + 58(470)] + [(470)(826) + (-826)(470)] && (19)\\ &= 2 + 0 = 2, && (20) \end{aligned}$$

so $(s_2, t_2) = \boxed{(437, -768)}$ works. $\boxed{(-503, 884)}$ also works. □

3. **Modular arithmetic**

(a) Evaluate $7^{500} \bmod 17$.

Solution. By repeated squaring, we have

$$\begin{aligned}
7^2 &\equiv 49 \equiv -2 \pmod{17} && (21)\\
7^4 &\equiv 4 \pmod{17} && (22)\\
7^8 &\equiv 16 \equiv -1 \pmod{17} && (23)\\
7^{16} &\equiv 1 \pmod{17} && (24)\\
7^{32} &\equiv 1 \pmod{17} && (25)\\
&\vdots && (26)
\end{aligned}$$

Thus,

$$7^{500} \equiv 7^{256+128+64+32+16+4} \equiv 7^{256}7^{128}7^{64}7^{32}7^{16}7^4 \equiv 4 \pmod{17}$$

and $7^{500} \bmod 17 = \boxed{4}$. Alternatively, Fermat's theorem tells us that $7^{16} \equiv 1 \pmod{17}$, so

$$7^{500} \equiv 7^{500 \bmod 16} \equiv 7^4 \equiv 4 \pmod{17}.$$

□

(b) Use Fermat's theorem to find a modulo 17 multiplicative inverse of 7.

Solution. By Fermat's theorem, we want $7^{15} \bmod 17$. Since

$$7^{15} \equiv 7^{8+4+2+1} \equiv 7^8 7^4 7^2 7 \equiv (-1)(4)(-2)(7) \equiv 56 \equiv 5 \pmod{17},$$

the answer is $\boxed{5}$. Indeed $(7)(5) \equiv 35 \equiv 1 \pmod{17}$. □

4. **Sets**

(a) Prove that if A, B, and C are sets, then $A-(B\cap C) \subseteq (A-B)\cup(A-C)$. (Note: To show that $S \subseteq T$, you must pick an arbitrary element of S and show that it is in T. A Venn diagram does not count as a proof.)

Solution. Suppose that $x \in A-(B\cap C)$. Then, $x \in A$ and $x \notin B \cap C$. By De Morgan's Law, this means that $x \notin B$ or $x \notin C$.
Case 1: $x \notin B$. Then, $x \in A-B$, so $x \in (A-B)\cup(A-C)$.
Case 2: $x \notin C$. Then, $x \in A-C$, so $x \in (A-B)\cup(A-C)$.
In both cases, $x \in (A-B)\cup(A-C)$, so $A-(B\cap C) \subseteq (A-B)\cup(A-C)$. □

(b) Let A and B be sets. Prove that $A \subseteq B$ if and only if $A-B=\emptyset$.

Solution. <u>($\Rightarrow$)</u>: We will prove the contrapositive. The contrapositive is: If $A-B \neq \emptyset$, then $A \not\subseteq B$. If $A-B \neq \emptyset$, then we can let $x \in A-B$. This means that $x \in A$ but $x \notin B$. This means that not every element in A is in B also, so $A \not\subseteq B$.
<u>($\Leftarrow$)</u>: Again, we will prove the contrapositive: If $A \not\subseteq B$, then $A-B \neq \emptyset$. If $A \not\subseteq B$, then not every element in A is also in B, so there must be some $x \in A$ such that $x \notin B$. Then, $x \in A-B$, so $A-B \neq \emptyset$. □

5. **Partial Order**

Let $A = \mathbb{Z}^2$, and define the relation R as follows: $(x_1, y_1)\, R\, (x_2, y_2)$ if

(a) $x_1 < x_2$, or

(b) $x_1 = x_2$ and $y_1 \le y_2$.

Show that R is a partial order.

Solution. We must show that R is reflexive, antisymmetric, and transitive.

- Reflexive: Suppose that $(x, y) \in A$. Since $x = x$ and $y \le y$, we have $(x, y)\, R\, (x, y)$, so R is reflexive.
- Antisymmetric: Suppose that $(x_1, y_1)\, R\, (x_2, y_2)$ and $(x_2, y_2)\, R\, (x_1, y_1)$. Then, $x_1 \le x_2$ and $x_2 \le x_1$. The only way this is possible is if $x_1 = x_2$. This means that $y_1 \le y_2$ and $y_2 \le y_1$. The only way this is possible is if $y_1 = y_2$. Thus, $(x_1, y_1) = (x_2, y_2)$, and R is antisymmetric.
- Transitive: Suppose that $(x_1, y_1)\, R\, (x_2, y_2)$ and $(x_2, y_2)\, R\, (x_3, y_3)$. Then, $x_1 \le x_2$ and $x_2 \le x_3$, so $x_1 \le x_3$. There are two cases:

  Case 1: $x_1 < x_3$. Then, $(x_1, y_1)\, R\, (x_3, y_3)$.

  Case 2: $x_1 = x_3$. Since $x_1 \le x_2 \le x_3$, this means that $x_1 = x_2 = x_3$. Hence, $y_1 \le y_2$ and $y_2 \le y_3$, so $y_1 \le y_3$. This means that $(x_1, y_1)\, R\, (x_3, y_3)$.

  In both cases, we have $(x_1, y_1)\, R\, (x_3, y_3)$, so R is transitive.

$\square$