Homework 8 Solutions

ECS 20 (Winter 2019)

Patrice Koehl
koehl@cs.ucdavis.edu

March 6, 2019

Exercise 1: (10 points)

Let a, b and n be three positive integers with $gcd(a, n) = 1$ and $gcd(b, n) = 1$. Show that $gcd(ab, n) = 1$

Let a, b, and n be three integers such that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$.
Since $\gcd(a, n) = 1$, according to Bezout's identity, there exist two integers k and l such that $ka + ln = 1$. Multiplying by b, we get $kab + lnb = b$.
Let $g = \gcd(ab, n)$. As g divides ab and n, there exists u and v such that $ab = ug$ and $n = vg$. Replacing in the equation above, we get $kgu + lvgb = b$, or $g(ku + lvb) = b$. Hence, g divides b. Since g also divides n, g is a common divisor of b and n. b and n being co-prime, the only possibility is $g = 1$, and therefore $\gcd(ab, n) = 1$, which concludes the proof.

Exercise 2 (10 points)

Prove that there are no solutions in integers x and y to the equation $2x^2+5y^2 = 14$. (Hint: consider this equation modulo 5)

We consider the equation $2x^2 + 5y^2 = 14$. Let us follow the hint:
Since $5 \equiv 0 (\text{mod } 5)$, $5y^2 \equiv 0 (\text{mod } 5)$. Hence $2x^2 + 5y^2 \equiv 2x^2 (\text{mod } 5)$.
Let us write $x = 5q + r$, with $0 \leq r \leq 4$. Then $x^2 = 25q^2 + 10q + r^2$, and therefore $x^2 \equiv r^2 (\text{mod } 5)$, and $2x^2 \equiv 2r^2 (\text{mod } 5)$. For $r = 0, 1, 2, 3, 4$, we get $2x^2 \equiv 0, 2, 3, 3, 2 (\text{mod } 5)$, respectively.
On the other hand, $14 \equiv 4 (\text{mod } 5)$. Therefore we cannot have $2x^2 + 5y^2 \equiv 14 (\text{mod } 5)$, and the equation does not have any solution.

Exercise 3 (total: 20 points)

Use Fermat's little theorem to evaluate:

(i) $2^{302} \mod 7$: Let us divide 302 by 7: 302 = 7*43+1. Then $2^{302} = 2^{7*43+1} = 2 * (2^{43})^7$.
Since 7 is prime, according to Fermat's little theorem, $(2^{43})^7 \equiv 2^{43} (\text{mod } 7)$, and therefore $2^{302} \equiv 2^{44} (\text{mod } 7)$.
Let us repeat the procedure: 44=7*6+2. Then $2^{44} = 2 * (2^6)^7$. Using Fermat's little theorem, we get $(2^6)^7 \equiv 2^6 (\text{mod } 7)$ and therefore $2^{44} \equiv 2^8 (\text{mod } 7)$.
According to Fermat's little theorem, $2^7 \equiv 2 (\text{mod } 7)$, and therefore $2^8 \equiv 4 (\text{mod } 7)$.
Combining all these, we conclude that $2^{302} \equiv 4 (\text{mod } 7)$.

(ii) 5^{123} mod 61: First, we know that 61 is prime. Let us divide 123 by 61: 123=2*61+1. Then $5^{123} = 5 * (5^2)^{61}$. According to Fermat's little theorem, $(5^2)^{61} \equiv 5^2 (\text{mod } 61)$, hence $5^{123} \equiv 5^3 (\text{mod } 61)$. Since $5^3 = 125 = 2*61+3$, $5^3 \equiv 3 (\text{mod } 61)$, and hence $5^{123} \equiv 3 (\text{mod } 61)$.

Exercise 4 (10 points)

Let n be an integer. Show that if $n > 3$ then n, $n+2$ and $n+4$ cannot all be prime

Let n be an integer. We consider the division of n by 3: there exists two integer k and r, with $r = 0, 1$ or 2, such that $n = 3k + r$. Let us consider the three cases:

a) $r = 0$ then $n = 3k$ and since $n > 3$, n is a multiple of 3 and is not prime.

b) $r = 1$ i.e. $n = 3k + 1$. Then, $n + 2 = 3k + 3 = 3(k + 1)$, which is not a prime.

c) $r = 2$, i.e. $n = 3k + 2$, then $n + 1 = 3k + 3 = 3(k + 1)$, is not a prime.

Therefore if n is greater than 3, n, $n + 2$ and $n + 4$ cannot all be prime.

Exercise 5 (total: 20 points)

Find the value of each of these sums:

There are two ways to solve these 4 problems: a systematic way, where we compute each term of the sequence explicitly, and sum them, or we use the closed forms for the sums of geometric sequences. Both are perfectly correct. Since I assume you have no problem with the first approach, I will describe the second. It is based on the property:

$$\sum_{i=0}^{N} ar^i = a\frac{r^{N+1} - 1}{r - 1} \quad if \quad r \neq 1$$
$$\sum_{i=0}^{N} ar^i = a(n+1) \quad if \quad r = 1$$

a)

$$\begin{aligned}\sum_{j=0}^{8}(1 + (-1)^j) &= \sum_{j=0}^{8} 1 + \sum_{j=0}^{8}(-1)^j \\ &= 9 + \frac{(-1)^9 - 1}{-1 - 1} \\ &= 9 + \frac{-1 - 1}{-1 - 1} \\ &= 10\end{aligned}$$

b)

$$\begin{aligned}\sum_{j=0}^{8}(3^j - 2^j) &= \sum_{j=0}^{8} 3^j - \sum_{j=0}^{8} 2^j \\ &= \frac{3^9 - 1}{3 - 1} - \frac{2^9 - 1}{2 - 1} \\ &= 9841 - 511 = 9330\end{aligned}$$

c)

$$\begin{aligned}\sum_{j=0}^{8}(2.3^j + 3.2^j) &= 2\sum_{j=0}^{8}3^j + 3\sum_{j=0}^{8}2^j \\ &= 2\frac{3^9-1}{3-1} + 3\frac{2^9-1}{2-1} \\ &= 2 * 9841 + 3 * 511 = 21215\end{aligned}$$

d)

$$\begin{aligned}\sum_{j=0}^{8}(2^{j+1} - 2^j) &= \sum_{j=0}^{8}2^j(2-1) \\ &= \sum_{j=0}^{8}2^j \\ &= \frac{2^9-1}{2-1} = 511\end{aligned}$$

Exercise 6 (10 points)

Using the identity $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$, *compute* $\sum_{k=1} n\frac{1}{k(k+1)}$

This is straightforward based on the hint that is provided:

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{k(k+1)} &= \sum_{k=1}^{n}(\frac{1}{k} - \frac{1}{k+1}) \\ &= \sum_{k=1}^{n}\frac{1}{k} - \sum_{k=1}^{n}\frac{1}{k+1}\end{aligned}$$

Making the change of indices $j = k + 1$ in the second sum, we get:

$$\begin{aligned}\sum_{k=1}^{n}\frac{1}{k(k+1)} &= \sum_{k=1}^{n}\frac{1}{k} - \sum_{j=2}^{n+1}\frac{1}{j} \\ &= \sum_{k=1}^{n}\frac{1}{k} - (\sum_{j=1}^{n}\frac{1}{j} + \frac{1}{n+1} - 1) \\ &= 1 - \frac{1}{n+1} \\ &= \frac{n}{n+1}\end{aligned}$$

Exercise 7 (10 points)

Without using mathematical induction, show that $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Let $S_1 = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $S_2 = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, and let $S_3 = \sum_{i=1}^{n} i^3$. As indicated in the hint, we compute $S = \sum_{i=1}^{n}(i+1)^4$ in 2 different ways:

a) We develop $(i+1)^4$:

$$\begin{aligned} S &= \sum_{i=1}^{n}(i+1)^4 \\ &= \sum_{i=1}^{n}(i^4+4i^3+6i^2+4i+1) \\ &= \sum_{i=1}^{n} i^4 + 4S_3 + 6S_2 + 4S_1 + n \end{aligned}$$

b) We make the change of variables $j = i+1$:

$$\begin{aligned} S &= \sum_{i=1}^{n}(i+1)^4 \\ &= \sum_{j=2}^{n+1} j^4 \\ &= \sum_{j=1}^{n} j^4 + (n+1)^4 - 1 \end{aligned}$$

Therefore,

$$\sum_{i=1}^{n} i^4 + 4S_3 + 6S_2 + 4S_1 + n = \sum_{j=1}^{n} j^4 + (n+1)^4 - 1$$

The sums of i^4 cancel out, and we get:

$$\begin{aligned} 4S_3 &= (n+1)^4 - 6S_2 - 4S_1 - n - 1 \\ &= n^4 + 4n^3 + 6n^2 + 4n + 1 - n(n+1)(2n+1) - 2n(n+1) - n - 1 \\ &= n^4 + 4n^3 + 6n^2 + 4n - (n^2+n)(2n+1) - 2n^2 - 2n - n \\ &= n^4 + 4n^3 + 6n^2 + 4n - 2n^3 - 3n^2 - n - 2n^2 - 3n \\ &= n^4 + 2n^3 + n^2 \\ &= n^2(n+1)^2 \end{aligned}$$

Therefore,

$$S_3 = \left(\frac{n(n+1)}{2}\right)^2$$

Exercise 8 (10 points)

Without using mathematical induction, prove that $\sum_{i=1}^{n} i(i+1)(i+2) = \frac{n(n+1)(n+2)(n+3)}{4}$ *for all integer* $n \geq 1$.

This problem is easy and can be solved using the results given in the previous problem (exercise 7). Using the notations from that problem, notice that

$$\begin{aligned}\sum_{i=1}^{n} i(i+1)(i+2) &= \sum_{i=1}^{n}(i^3+3i^2+2i)\\ &= S_3+3S_2+2S_1\end{aligned}$$

where $S_1=\sum_{i=1}^{n} i=\frac{n(n+1)}{2}$, $S_2=\sum_{i=1}^{n} i^2=\frac{n(n+1)(2n+1)}{6}$, and $S_3=\sum_{i=1}^{n} i^3=\left(\frac{n(n+1)}{2}\right)^2$.
Therefore

$$\begin{aligned}\sum_{i=1}^{n} i(i+1)(i+2) &= \frac{n^2(n+1)^2}{4}+\frac{n(n+1)(2n+1)}{2}+\frac{n(n+1)}{2}\\ &= \frac{n^2(n+1)^2+2n(n+1)(2n+1)+4n(n+1)}{4}\\ &= \frac{n(n+1)[n(n+1)+2(2n+1)+4]}{4}\\ &= \frac{n(n+1)[n^2+5n+6]}{4}\\ &= \frac{n(n+1)(n+2)(n+3)}{4}\end{aligned}$$

Extra credit (3 points)

Let a and b be two natural numbers.

a) *Show that if $gcd(a,b)=1$ then $gcd(a+b,ab)=1$*

We use a proof by contradiction. We suppose that there exists two natural numbers a and b such that $gcd(a,b)=1$ and $gcd(a+b,ab)\neq 1$.

Since $gcd(a+b,ab)\neq 1$, there exists a natural number k, with $k>1$ such that $k=gcd(a+b,ab)$. Since $k>1$, according to the fundamental theorem of arithmetics, it can be written as a product of prime number. Let p be one of the prime numbers. We have p/k, and since k/ab, p/ab. Since p is prime and p/ab, according to Euclid's theorem, p/a or p/b.

If p/a, since $p/(a+b)$, $p/(a+b)-a$, therefore p/b. Similarly, If p/b, since $p/(a+b)$, $p/(a+b)-b$, therefore p/a.

In all cases, we have that p/a and p/b. Therefore $p\leq gcd(a,b)$, but $gcd(a,b)=1$. This is a contradiction as p is prime. Therefore the property is true.

b) *Show that if $gcd(a,b)=1$ then $gcd(a^2+b^2,ab)=1$*

We use a direct proof. Based on part a), as $gcd(a,b)=1$, we have $gcd(a+b,ab)=1$. According to Bezout's identity, there exists two integers l and m such that

$$(a+b)l+abm=1$$

Squaring this equation, we get:

$$(a^2+b^2)l^2+(ab)^2m^2+2abl=1$$

Now, let $h = gcd(a^2 + b^2, ab)$. Then $h/(a^2 + b^2)$ and h/ab. There exists two integers u and v such that $a^2 + b^2 = hu$ and $ab = hv$. Replacing in the equation above, we get:

$$hul^2 + h^2v^2m^2 + 2hvl = 1$$

i.e.

$$h(ul^2 + hv^2m^2 + 2vl) = 1$$

This means that $h/1$, and therefore $h = 1$.