Math 55—Fall 2025—Haiman
Homework 4

Due on Gradescope Wednesday, Sept. 24, 8pm

Problems from Rosen

Section 4.1

4. Prove (iii) if $a|b$ and $b|c$, then $a|c$

   Answer: Suppose that $a|b$ *and* $b|c$*, then it follows that* $b = ka$ *for some integer* k *and* $c = nb$ *for some integer* n*. Since we can write* b *as* ka *for some integer* k*, we can also write* $c = nk * a$ *for some integer* n *and some integer* k*, therefore* a *divides* c*,* $(a|c)$*.*

10. Prove that if a and b are nonzero integers, a divides b, and a + b is odd, then a is odd.

    Answer: Suppose $b = ma$ *for some* $m \in \mathbb{Z}$*, and* $a + b \,(mod\, 2) \equiv 1$ *so that* $a + b = 2k + 1$ *for some integer* k*. It follows that:*

    $$a + b = a + ma = a\,(m + 1) = 2k + 1$$

    An odd number cannot be divisible by an even number, because any multiple of an even number is even. If a *was even, then* $a + b = a\,(m + 1)$ *is also even as* $(m+1) \in \mathbb{Z}$*, which contradicts the given premise that* $a+b$ *is odd. Therefore* a *must be an odd number.*

18. (f) Try to do it without calculating the integer $113+4 \cdot 33$. Suppose that a and b are integers, $a \equiv 11\,(mod\, 19)$, and $b \equiv 3\,(mod\, 19)$. Find the integer c with $0 \leq c \leq 18$ such that:

    (f) $c \equiv a^3 + 4b^3\,(mod\, 19)$

    Answer: Use the theorem If $a \equiv b\,(mod\, m)$ *and* $c \equiv d\,(mod\, m)$*,*
    then 1.) $\boldsymbol{a + c \equiv b + d\,(mod\, m)}$ *and 2.)* $\boldsymbol{ac \equiv bd\,(mod\, m)}$*.*

    $$a^3 \equiv 11^3 \equiv 11 \times 11^2\,(mod\, 19) \equiv 11 \times 7\,(mod\, 19) \equiv 1\,(mod\, 19)$$

    $$b^3\,(mod\, 19) \equiv 27\,(mod\, 19) \equiv 8\,(mod\, 19)$$

    $$4 \times 8\,(mod\, 19) \equiv 32\,(mod\, 19) \equiv 13\,(mod\, 19)$$

    $$c \equiv 13 + 1\,(mod\, 19)$$

    $$c = 14\,(mod\, 19)$$

42. Show that if a, b, c,and m are integers such that $m \geq 2$, $c \geq 0$, and $a \equiv b\,(mod\,m)$, then $ac \equiv bc\,(mod\,mc)$.

Answer: $a \equiv b\,(mod\,m) \implies m \,|\, (a-b)$. *In other words, there exist an integer* k *such that* $a - b = km$.
If we multiply both sides by c*, we get* $c(a-b) = ckm$.
It follows that:

$$c\,(a-b) \equiv ckm\,(mod\,mc)$$

$$\implies ac - bc \equiv ckm\,(mod\,mc)$$

$$\implies ac - bc \equiv 0\,(mod\,mc)$$

$$\therefore\ ac \equiv bc\,(mod\,mc)$$

Section 4.3

6. How many zeros are there at the end of 100!?
Note: $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$ is defined to be the product of the integers 1 through n.

Hint: as a warm-up, try it for 10! *first using the answer to Exercise 5.*

The prime factorization of 10! *is* $2^8 + 3^4 + 5^2 + 71$. *The tail zeros come from the factors that have a product of10, which can only be prime factorized by 2 and 5. As there are more 2s than 5s, we only want to count how many 5s there are. Since there are two 5s, there are two zeros at the end of* 10!.

Answer: We want to count the prime factors 2^n *and* 5^k*, where* $0 \leq k \leq n$. *We want to count the number of times the prime 5 appears in the prime factorization of n!. Trailing zeros come from factors of* $10 = 2 \times 5$*, and there are always more 2s than 5s in* n! *Every multiple of 5 contributes 1 factor of 5 in the prime factorization, while every multiple of 25 contributes 2 factors of 5 in the prime factorization. That is, 5, 10, ... , 100 all contribute one 5 to the prime factorization, and 25, 50, 75, 100 contribute an extra 5. Therefore there are*

$$\frac{100}{5} + \frac{100}{25} = 24$$

24 factors of 5 in the prime factorization of 100!. *Hence there are 24 zeros at the end of 10 factorial.*

12. Prove that for every positive integer n, there are n consecutive composite integers. [Hint: Consider the n consecutive integers starting with $(n+1)! + 2$.]

Answer: Composite integers are positive integers greater than 1 that are not prime, meaning they have factors other than just 1 and themselves.
Let $n \in \mathbb{Z}^+$*, and* N *be* $(n-1)!$. *Consider* n *consecutive integers N+2,*

N+3, ... , N + (n+1).
For each $k \in \{2, 3, 4, ..., n+1\}$*:*

$$k \mid (n+1)! \implies k \mid N \implies k \mid N + k$$

Since N + k has proper divisor k, it is always composite. The cardinality of the set {2, 3, ... , n+1} is n, so there are n consecutive positive integers N+2, N+3, ..., N + (n+1) for every positive integer n.

16. Determine whether the integers in each of these sets are pairwise relatively prime.

    a) 21, 34, 55
    Answer: $gcd(21, 34) = gcd(21, 55) = gcd(34, 55) = 1$*, so the integers in this set are pairwise relatively prime.*
    b) 14, 17, 85
    Answer: $gcd(14, 17) = 1$*,* $gcd(14, 85) = 1$*, but* $gcd(17, 85) = 17 > 1$*. Therefore this set of integers are not relatively prime.*

18. We call a positive integer perfect if it equals the sum of its positive divisors other than itself.
    FYI: A theorem of Euler says that every even perfect number is of the type in part (b). It is not known whether there are any odd perfect numbers, or whether there are infinitely many perfect numbers.

    a) Show that 6 and 28 are perfect.

    Answer: 6 has positive divisors 1, 2, 3, where $1+2+3 = 6$*, so 6 is a perfect integer. 28 has positive divisors 1, 2, 4, 7, 14, and* $1+2+4+7+14 = 28$

    b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

    Answer: Let $M = 2^p - 1$ *be prime and* $N = 2^{p-1}M$*. The positive divisors of* N *are exactly* 2^k *and* 2^kM *for* $0 \leq k \leq p-1$ *as* M *is prime and odd. Therefore*

$$\sigma(N) = \sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-1} 2^k M = \left(\sum_{k=0}^{p-1} 2^k\right)(1+M) = (2^p-1)(1+2^p-1) = (2^p-1)2^p = 2N,$$

    hence N *is perfect.*

24. What are the greatest common divisors of these pairs of integers? (26) What is the least common multiple of each pair in Exercise 24?

    b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, \quad 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

    Answer: $\text{gcd} = 2 \cdot 3 \cdot 11 = 66$. $\quad \text{lcm} = 2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$.

    d) $2^2 \cdot 7, \quad 5^3 \cdot 13$

    Answer: $\text{gcd} = 1$. $\quad \text{lcm} = 2^2 \cdot 7 \cdot 5^3 \cdot 13 = 45{,}500$.

    e) 0, 5

    Answer: $\text{gcd}(0, 5) = 5$. $\quad \text{lcm}(0, 5) = 0$.

28. Find $gcd\,(1000, 625)$ and $lcm\,(1000, 625)$ and verify that $gcd\,(1000, 625) \cdot lcm\,(1000, 625) = 1000 \cdot 625$.

Answer: Prime factorizations:

$$1000 = 2^3 \cdot 5^3, \qquad 625 = 5^4.$$

Hence

$$\gcd(1000, 625) = 5^3 = 125, \qquad \mathrm{lcm}(1000, 625) = 2^3 \cdot 5^4 = 5000.$$

Verification:

$$\gcd(1000, 625) \cdot \mathrm{lcm}(1000, 625) = 125 \cdot 5000 = 625000 = 1000 \cdot 625.$$