

MATH 230
STUDY GUIDE FOR MIDTERM 1

(1) Find, and prove by induction, a formula for

$$1^3 + 4^3 + 7^3 + 10^3 + \cdots + (3n + 1)^3.$$

There are several strategies for finding a formula. The most straightforward is to algebraically manipulate known formulas for sums of powers of integers:

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}; \quad \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}; \quad \sum_{k=1}^n k^3 = \frac{n^2(n+1)^2}{4}.$$

Then

$$\begin{aligned} \sum_{k=0}^n (3k+1)^3 &= \sum_{k=0}^n (27k^3 + 27k^2 + 9k + 1) \\ &= 27 \sum_{k=0}^n k^3 + 27 \sum_{k=0}^n k^2 + 9 \sum_{k=0}^n k + \sum_{k=0}^n 1 \\ &= \frac{27n^2(n+1)^2}{4} + \frac{27n(n+1)(2n+1)}{6} + \frac{9n(n+1)}{2} + (n+1) \\ &= \frac{27n^4 + 90n^3 + 99n^2 + 40n + 4}{4}. \end{aligned}$$

Now we'll prove this formula by induction. First, we verify the base case, $n = 0$:

$$\frac{(0+1)(3 \cdot 0 + 2)(9 \cdot 0^2 + 15 \cdot 0 + 2)}{4} = 1 = 1^3.$$

Now let's assume the proposition for n :

$$\sum_{k=0}^n (3k+1)^3 = \frac{27n^4 + 90n^3 + 99n^2 + 40n + 4}{4}.$$

Adding $(3(n+1)+1)^3 = (3n+4)^3$ to both sides, we obtain

$$\begin{aligned} \sum_{k=0}^{n+1} (3k+1)^3 &= \frac{27n^4 + 90n^3 + 99n^2 + 40n + 4}{4} + (3n+4)^3 \\ &= \frac{27n^4 + 90n^3 + 99n^2 + 40n + 4}{4} + \frac{108n^3 + 432n^2 + 576n + 256}{4} \\ &= \frac{27n^4 + 198n^3 + 531n^2 + 616n + 260}{4}. \end{aligned}$$

On the other hand,

$$\begin{aligned} &\frac{27(n+1)^4 + 90(n+1)^3 + 99(n+1)^2 + 40(n+1) + 4}{4} \\ &= \frac{27(n^4 + 4n^3 + 6n^2 + 4n + 1) + 90(n^3 + 3n^2 + 3n + 1) + 99(n^2 + 2n + 1) + 40(n+1) + 4}{4} \\ &= \frac{27n^4 + 198n^3 + 531n^2 + 616n + 260}{4}. \end{aligned}$$

Thus the proposition for $n+1$ follows from the inductive hypothesis, and the statement is proved by induction.

- (2) Give the prime factorization of each of the following integers.

For the first four, we just use trial division:

(a) $341 = 11 \cdot 13$

(b) $343 = 7 \cdot 49 = 7^3$

(c) $345 = 3 \cdot 115 = 3 \cdot 5 \cdot 23$

(d) 347 is prime, which we can verify by checking divisibility by the primes up through 17, since $19^2 = 361 > 347$.

(e) $27!$

For $27!$, we work prime by prime.

There are 13 even numbers between 1 and 27, of which 6 are divisible by 4, 3 are divisible by 8, and 1 is divisible by 16. Thus the power of 2 in the prime factorization of $27!$ is $13+6+3+1 = 23$.

There are 9 numbers between 1 and 27 that are divisible by 3, of which 3 are divisible by 9, and 1 is divisible by 27. Thus the power of 3 in the prime factorization of $27!$ is $9+3+1 = 13$.

There are 5 numbers between 1 and 27 that are divisible by 5, of which 1 is divisible by 25. Thus the power of 5 in the prime factorization of $27!$ is $5+1 = 6$.

There are 3 numbers between 1 and 27 that are divisible by 7; 2 that are divisible by 11; and 2 that are divisible by 13. Thus the powers of 7, 11, and 13 in the prime factorization of $27!$ are 3, 2, and 2, respectively.

For each of the primes 17, 19, and 23, there is just one number between 1 and 27 that is divisible by it; thus, their powers in the prime factorization of $27!$ are each 1.

No prime larger than 27 occurs in the prime factorization of $27!$, since it does not divide any of the factors.

Putting this all together, we obtain the factorization

$$27! = 2^{23} \cdot 3^{13} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23.$$

(f) $\binom{46}{21} = \frac{46!}{21!25!}$

We argue as above to obtain the prime factorizations

$$46! = 2^{42} \cdot 3^{21} \cdot 5^{10} \cdot 7^6 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43$$

$$21! = 2^{18} \cdot 3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

$$25! = 2^{22} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$

Dividing the first by the latter two, we obtain

$$\binom{46}{21} = 2^2 \cdot 3^2 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43.$$

(3) Let $n = 1260$.

(a) Find the prime factorization of n .

$$n = 20 \cdot 63 = 2^2 \cdot 3^2 \cdot 5 \cdot 7.$$

(b) Find the number of divisors of n , $d(n)$.

We use the fact that

$$d(p_1^{a_1} p_2^{a_2} \cdots) = (a_1 + 1)(a_2 + 1) \cdots.$$

So in this case,

$$d(n) = d(2^2 \cdot 3^2 \cdot 5 \cdot 7) = 3 \cdot 3 \cdot 2 \cdot 2 = 36.$$

(c) Find the sum of the divisors of n , $\sigma(n)$. We use the fact that

$$\sigma(p_1^{a_1} p_2^{a_2} \cdots) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots.$$

So in this case,

$$\begin{aligned} \sigma(n) &= \sigma(2^2 \cdot 3^2 \cdot 5 \cdot 7) \\ &= \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} \\ &= \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} \cdot \frac{48}{6} \\ &= 7 \cdot 13 \cdot 6 \cdot 8 = 4368. \end{aligned}$$

(d) Find the smallest number with more divisors than n .

(i) Since 37 is prime, the smallest number with 37 divisors is 2^{36} .

(ii) Since $38 = 2 \cdot 19$, the smallest number with 38 divisors could be of the form p^{37} or of the form $p^{18}q$. Since $2^{18} \cdot 3 < 2^{37}$, the smallest number with 38 divisors is $2^{18} \cdot 3$, which is better than the number found in (a).

(iii) Since $39 = 3 \cdot 13$, the smallest number with 39 divisors could be of the form p^{38} or of the form $p^{12}q^2$. Since $2^{12} \cdot 3^2 < 2^{38}$, the smallest number with 39 divisors is $2^{12} \cdot 3^2$, which is better than the number found in (b).

(iv) Since $40 = 2 \cdot 2 \cdot 2 \cdot 5$, there are several possibilities for the form of the smallest number with 40 divisors:

$$\begin{aligned} 40 &\rightarrow 2^{39} \\ 2 \cdot 20 &\rightarrow 2^{19} \cdot 3 \\ 4 \cdot 10 &\rightarrow 2^9 \cdot 3^3 \\ 5 \cdot 8 &\rightarrow 2^7 \cdot 3^4 \\ 2 \cdot 2 \cdot 10 &\rightarrow 2^9 \cdot 3 \cdot 5 \\ 2 \cdot 4 \cdot 5 &\rightarrow 2^4 \cdot 3^3 \cdot 5 \\ 2 \cdot 2 \cdot 2 \cdot 5 &\rightarrow 2^4 \cdot 3 \cdot 5 \cdot 7 \end{aligned}$$

By inspection, the smallest of these is the last one, 1680.

Showing that 1680 is the smallest number with more than 36 divisors is significantly more difficult, and requires the consideration of a large number of cases or a computer search.

(4) Let $a = 397$ and $b = 341$.

(a) Find the greatest common divisor of a and b .

We use the Euclidean Algorithm.

$$397 = 1 \cdot 341 + 56$$

$$341 = 6 \cdot 56 + 5$$

$$56 = 11 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0$$

Thus $\gcd(397, 341) = 1$.

(b) Do there exist natural numbers x and y such that $ax - by = 1$? If so, find such a pair (x, y) .

Yes, 1 is a linear combination of 397 and 341, since they are relatively prime. To find a pair, we reverse the steps of the Euclidean Algorithm:

$$1 = 56 - 11 \cdot 5$$

$$= 56 - 11(341 - 6 \cdot 56)$$

$$= 67 \cdot 56 - 11 \cdot 341$$

$$= 67(397 - 341) - 11 \cdot 341$$

$$= 67 \cdot 397 - 78 \cdot 341.$$

So we can take $x = 67$ and $y = 78$.

(c) Do there exist natural numbers x and y such that $ax - by = 6$? If so, find such a pair (x, y) .

Yes, we can just multiply the equation from part (a) by 6, to obtain $x = 402$ and $y = 468$. A smaller solution is given by $x = 402 - 341 = 61$ and $y = 468 - 397 = 71$.

(d) Do there exist natural numbers x and y such that $by - ax = 1$? If so, find such a pair (x, y) .

Yes, we can adapt our answer from part (a): take $x = 341 - 67 = 274$ and $y = 397 - 78 = 319$.

(5) Do the following calculations in modular arithmetic.

(a) $1 + 2 + 3 + \cdots + 100 \pmod{101}$

$$1 + 2 + 3 + \cdots + 100 = \frac{100(101)}{2} \equiv 0 \pmod{101}.$$

(b) $\frac{1}{8} \pmod{13}$

$$\frac{1}{8} \equiv \frac{-12}{8} \equiv \frac{-3}{2} \equiv \frac{10}{2} \equiv 5 \pmod{13}.$$

Alternatively, one could use the extended Euclidean Algorithm on the pair $(8, 13)$ to find

$$1 = 5 \cdot 8 - 3 \cdot 13,$$

from which it follows that $\frac{1}{8} \equiv 5 \pmod{13}$.

(c) $\frac{3}{5} \pmod{31}$

$$\frac{3}{5} = 3 \cdot \frac{1}{5} \equiv 3 \cdot \frac{-30}{5} \equiv 3(-6) \equiv -18 \equiv 13 \pmod{31}.$$

Alternatively, one could use the extended Euclidean Algorithm on the pair $(5, 31)$ to find

$$1 = 1 \cdot 31 - 6 \cdot 5,$$

from which it follows that $\frac{1}{5} \equiv -6 \equiv 25 \pmod{31}$, and $\frac{3}{5} \equiv 3 \cdot 25 \equiv 75 \equiv 13 \pmod{31}$.

(d) $2^{14} \pmod{15}$

Note that since 15 is not prime, Fermat's Theorem does not apply. But $2^4 = 16 \equiv 1 \pmod{15}$, so

$$2^{14} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^2 \equiv 2^2 \equiv 4 \pmod{15}.$$

(e) $3^{78} \pmod{17}$

By Fermat's Theorem, $3^{16} \equiv 1 \pmod{17}$, so

$$3^{78} = \frac{(3^{16})^5}{3^2} \equiv \frac{1}{9} \equiv \frac{18}{9} \equiv 2 \pmod{17}.$$

(f) $100! \pmod{103}$

By Wilson's Theorem, $102! \equiv -1 \pmod{103}$, since 103 is prime. Thus

$$102 \cdot 101 \cdot 100! \equiv -1 \pmod{103},$$

from which it follows that

$$100! \equiv \frac{-1}{102 \cdot 101} \equiv \frac{-1}{(-1)(-2)} \equiv -\frac{1}{2} \equiv -\frac{104}{2} \equiv -52 \equiv 51 \pmod{103}.$$

(g) $100! \pmod{105}$

Since $100! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdots 100$, and $105 = 3 \cdot 5 \cdot 7$, it's clear that $100!$ is divisible by 105, and hence $100! \equiv 0 \pmod{105}$.

(6) Define $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, so that F_n denotes the n^{th} Fibonacci number.

(a) Show that if $m \mid n$, then $F_m \mid F_n$.

Our approach will be similar to the one we used in showing that if $5 \mid n$, then $5 \mid F_n$. Specifically, let's compute:

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &= (F_{n-2} + F_{n-3}) + F_{n-2} = 2F_{n-2} + F_{n-3} \\ &= 2(F_{n-3} + F_{n-4}) + F_{n-3} = 3F_{n-3} + 2F_{n-4} \\ &= 3(F_{n-4} + F_{n-5}) + 2F_{n-4} = 5F_{n-4} + 3F_{n-5} \end{aligned}$$

At this point, when we were investigating when $5 \mid F_n$, we stopped. But after a few more steps, a pattern emerges:

$$\begin{aligned} F_n &= 5F_{n-4} + 3F_{n-5} \\ &= 5(F_{n-5} + F_{n-6}) + 3F_{n-5} = 8F_{n-5} + 5F_{n-6} \\ &= 8(F_{n-6} + F_{n-7}) + 5F_{n-6} = 13F_{n-6} + 8F_{n-7} \end{aligned}$$

It seems that $F_n = F_{m+1}F_{n-m} + F_mF_{n-m-1}$. We'll prove this lemma by induction on m .

When $m = 0$, the proposition is $F_n = F_1F_n + F_0F_{n-1}$, which is true since $F_1 = 1$ and $F_0 = 0$.

Now we'll assume the proposition for m :

$$F_n = F_{m+1}F_{n-m} + F_mF_{n-m-1}.$$

Since $F_{n-m} = F_{n-m-1} + F_{n-m-2}$, we obtain

$$\begin{aligned} F_n &= F_{m+1}(F_{n-m-1} + F_{n-m-2}) + F_mF_{n-m-1} \\ &= (F_{m+1} + F_m)F_{n-m-1} + F_{m+1}F_{n-m-2} \\ &= F_{m+2}F_{n-m-1} + F_{m+1}F_{n-m-2} \end{aligned}$$

This is exactly the statement of the proposition for $m + 1$, so this completes the proof by induction.

Now if $m \mid n$, then $n = km$ for some natural number k . We'll prove that $F_m \mid F_n$ by induction on k .

When $k = 1$, the assertion is $F_m \mid F_m$, which is trivially true.

Now assume the inductive hypothesis, that $F_m \mid F_{km}$. We'd like to show that $F_m \mid F_{(k+1)m}$.

By the lemma,

$$F_{(k+1)m} = F_{m+1}F_{km} + F_mF_{km-1}.$$

Since $F_m \mid F_{km}$ by the inductive hypothesis, F_m divides both terms in this sum, and so $F_m \mid F_{k+1}m$, and the statement is proved by induction.

(b) Show that if F_n is prime, then $n = 4$ or n is prime.

Since $m \mid n$ implies $F_m \mid F_n$, if n has a factor m such that $1 < F_m < F_n$, then F_n is composite.

Since $F_m > 1$ if $m > 2$, every composite number greater than 4 has such a factor m , which proves the assertion.

(c) If $n \geq 3$ is prime, is F_n necessarily prime?

As it turns out, the converse is false. The first counterexample is

$$F_{19} = 4181 = 37 \cdot 113.$$