Algebra I

Winter 2020

WAYNE STATE UNIVERSITY

1.1 Divisors

1. Let $m, n.r.s \in \mathbb{Z}$. If $m^2 + n^2 = r^2 + s^2 = mr + ns$, prove that $m = r$ and $n = s$.

Joe Starr

We select $m, n.r.s \in \mathbb{Z}$, given $m^2 + n^2 = r^2 + s^2 = mr + ns$ which can write as $m^2 + n^2 - mr - ns = r^2 + s^2 - mr - ns$. From here we can simplify:

$$\begin{aligned} m^2 + n^2 - mr - ns = r^2 + s^2 - mr - ns &\Rightarrow m\left(m - r\right) + n\left(n - s\right) = r\left(r - m\right) + s\left(s - n\right) \\ &\Rightarrow m\left(m - r\right) + n\left(n - s\right) - r\left(r - m\right) - s\left(s - n\right) = 0 \\ &\Rightarrow m\left(m - r\right) + r\left(m - r\right) + n\left(n - s\right) + s\left(n - s\right) = 0 \\ &\Rightarrow \left(m - r\right)\left(m + r\right) + \left(n - s\right)\left(n + s\right) = 0 \end{aligned}$$

from here we can see that in order for $\left(m - r\right)\left(m + r\right) + \left(n - s\right)\left(n + s\right) = 0$ to be true $m = r$ and $n = s$.

3. Find the quotient and reminder when a id divided by b.

a $a = 99$, $b = 17$

b $a = -99$, $b = 17$

c $a = 17$, $b = 99$

d $a = -1017$, $b = 99$

Joe Starr

a $99 = 17q + r \Rightarrow q = 5, r = 14$

b $-99 = 17q + r \Rightarrow q = -6, r = 3$

c $17 = 99q + r \Rightarrow q = 0, r = 17$

d $-1017 = 99q + r \Rightarrow q = -11, r = 72$

5. Use the Euclidean algorithm to find the following greatest common divisors

a $(6643, 2873)$

b $(7684, 4148)$

c $(26460, 12600)$

d $(6540, 1206)$

e $(12091, 8439)$

Joe Starr

(a) $(6643, 2873)$

$$6643 = 2873 * 2 + 897$$
$$2873 = 897 * 3 + 182$$
$$897 = 182 * 4 + 169$$
$$182 = 169 * 1 + 13$$
$$169 = 13 * 13$$

(b) $(7684, 4148)$

$$7684 = 4148 * 1 + 3536$$
$$4148 = 3536 * 1 + 612$$
$$3536 = 612 * 5 + 476$$
$$612 = 476 * 1 + 136$$
$$476 = 136 * 3 + 68$$
$$136 = 68 * 68$$

(c) $(26460, 12600)$

$$26460 = 12600 * 2 + 1260$$
$$12600 = 1260 * 10$$

(d) $(6540, 1206)$

$$\begin{aligned}
6540 &= 1206 * 5 + 510 \\
1206 &= 510 * 2 + 186 \\
510 &= 186 * 2 + 138 \\
186 &= 138 * 1 + 48 \\
138 &= 48 * 2 + 42 \\
48 &= 42 * 1 + 6 \\
42 &= 6 * 7
\end{aligned}$$

(e) $(12091, 8439)$

$$\begin{aligned}
12091 &= 8439 * 1 + 3652 \\
8439 &= 3652 * 2 + 1135 \\
3652 &= 1135 * 3 + 247 \\
1135 &= 247 * 4 + 147 \\
247 &= 147 * 1 + 100 \\
147 &= 100 * 1 + 47 \\
100 &= 47 * 2 + 6 \\
47 &= 6 * 7 + 5 \\
6 &= 5 * 1 + 1 \\
5 &= 1 * 5
\end{aligned}$$

7. For each part of Exercise 5, find integers m and n such that (a, b) is expressed in the form $ma + nb$.

Joe Starr

(a) $(6643, 2873)$

$$(6643) - 16 + (2873)\,37 = 13$$

(b) $(7684, 4148)$

$$(7684)\,27 + (4148) - 50 = 68$$

(c) $(26460, 12600)$ $(26460)\,1 + (12600) - 2 = 1260$

(d) $(6540, 1206)$ $(6540) - 26 + (1206)\,141 = 6$

(e) $(12091, 8439)$ $(12091)\,1435 + (8439) - 2056 = 1$

9. let a, b, c be integers such that $a+b+c=0$. Show that if n is an integer which is a divisor of two of the three integers, then it is also a divisor of the third.

Joe Starr

Select $a, b, c \in \mathbb{Z}$ to satisfy $a+b+c=0$, WLOG let $n \in \mathbb{Z}$ such that $n|a$ and $n|b$. Since $(a+b)+c=0$ it must be that $(a+b)=-c$. From here we must show $n|(a+b)$, or $a+b=nq$. Since $n|a$ and $n|b$ we may write $a=nq_1$ and $b=nq_2$, yielding, $nq_1+nq_2=n\left(q_1+q_2\right)=nq$ thus $n|c$, as desired.$\square$

13. Show that if n is any integer, then $(10n_3, 5n + 2) = 1$

Joe Starr

We begin with the Euclidean algorithm,

$$10n + 3 = (5n + 2)\,1 + (5n + 1)$$

$$5n + 2 = (5n + 1)\,1 + 1$$

from here we have $(10n + 3, 5n + 2) = (5n + 2, 5n + 1) = 1$, as desired.

15. For what positive integers n is it true that $(n, n+2) = 2$? Prove your claim.

Joe Starr

The conjecture is that the statement is true for even values of n. We begin with rewriting n in terms of k, $n = 2k$the Euclidean algorithm,

$$(2k) + 2 = (2k)\,1 + (2)$$

$$2k = (2)\,k$$

from here we have $(n+2, n) = (2k+2, 2k) = 2$, as desired.

17. Show that the positive integer k is the difference of two odd squares if and only if k is divisible by 8.

Joe Starr

We begin by writing $k = a^2 - b^2$, since a and b are odd we can write,

$$a = 2r + 1$$

$$b = 2s + 1$$

from here we have $q^2 - b^2 = 4(r + s + 1)(r - s)$. Since $k > 0$ we must consider two cases $r - s = 2m + 1$ and $r - s = 2m$.

$r - s = 2m$:

In this case we have $q^2 - b^2 = 4(r + s + 1) 2m = 8(r + s + 1) m$ and we are done.

$r - s = 2m + 1$:

In this case we have $r - s = 2m + 1$ and $r + s = r - s + 2s = 2m + 1 + 2s$

$$
\begin{aligned}
q^2 - b^2 &= 4\left(r + s + 1\right)\left(2m + 1\right) \\
&= 4\left(2m\left(r + s + 1\right) + \left(r + s + 1\right)\right) \\
&= 4\left(\left(2mr + 2ms + 2m\right) + \left(r + s + 1\right)\right) \\
&= 4\left(2mr + 2ms + 2m + r + s + 1\right) \\
&= 4\left(2mr + 2ms + 2m + 2m + 1 + 2s + 1\right) \\
&= 4\left(2mr + 2ms + 2m + 2m + 2s + 2\right) \\
&= 8\left(mr + ms + m + m + s + 1\right)
\end{aligned}
$$

as desired.

1.2 Primes

1. Find the prime factorizations of each of the following numbers, and use the them to compute the greatest common divisor and least common multiple of the given pairs of numbers.

(a) $(35, 14)$

(b) $(15, 11)$

(c) $(252, 11)$

(d) $(7684, 4148)$

(e) $(6643, 2873)$

Joe Starr

(a) $(35, 14)$

$35 : 5, 7$

$14 : 2, 7$

gcd: 7

lcm: 70

(b) $(15, 11)$

$15 : 3, 5$

$11 : 11$

gcd: 1

lcm: 165

(c) $(252, 180)$

$252 : 2, 2, 3, 3, 7$

$180 : 2, 2, 3, 3, 5$

gcd: 36

lcm: 1260

(d) $(7684, 4148)$

$7684 : 2, 2, 17, 113$

$4148 : 2, 2, 17, 61$

gcd: 68

lcm: 468724

(e) $(6643, 2873)$

$6643 : 7, 13, 73$

$2873 : 13, 13, 17$

gcd: 13

lcm: 1468103

2. US the sieve of Eratosthenes to find all prime numbers less than 200.

Joe Starr

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

3. For each composite number a. with $4 \leq a \leq 20$, find all positive numbers less than a that are relatively prime to a.

Joe Starr

$4: \ 2, 3$

$6: \ 2, 3, 5$

$8: \ 2, 3, 5, 7$

$9: \ 2, 3, 4, 5, 7, 8$

$10: \ 2, 3, 5, 7, 9$

$12: \ 2, 3, 5, 7, 11$

$14: \ 2, 3, 5, 7, 9, 11, 13$

$15: \ 2, 3, 4, 5, 7, 8, 11, 13, 14$

$16: \ 2, 3, 5, 7, 9, 11, 13, 15$

$18: \ 2, 3, 5, 7, 11, 13, 17$

$20: \ 2, 3, 5, 7, 9, 11, 13, 17, 19$

4. Find all positive integers less than 60 and relatively prime to 60.

Joe Starr

$60: \ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59$

9. (a) For which $n \in \mathbb{Z}^+$ is $n^3 - 1$ a prime number?

(b) For which $n \in \mathbb{Z}^+$ is $n^3 + 1$ a prime number?

(c) For which $n \in \mathbb{Z}^+$ is $n^2 - 1$ a prime number?

(d) For which $n \in \mathbb{Z}^+$ is $n^2 + 1$ a prime number?

Joe Starr

(a) We can factor $n^3 - 1$ into $(n-1)(n^2+n+1)$. We have then $n-1|n^3-1$, for n^3-1 to be prime $n-1$ must be 1. This happens only for $n = 2$.

(b) We can factor $n^3 + 1$ into $(n+1)(n^2 - n + 1)$. We have then $(n^2 - n + 1)|n^3 + 1$, for $n^3 + 1$ to be prime $(n^2 - n + 1)$ must be 1. This happens only for $n = 1$.

(c) We can factor $n^2 - 1$ into $(n-1)(n+1)$. We have then $(n11)|n^2 - 1$, for $n^2 - 1$ to be prime $(n - 1)$ must be 1. This happens only for $n = 2$. For which $n \in \mathbb{Z}^+$ is $n^2 - 1$ a prime number?

(d) ????

11. Prove that $n^4 + 4^n$ is composite if $n > 1$.

Joe Starr

We are presented with two potability's, n is even or n is odd.

n even

It's obvious that $n^4 + 4^n$ is an even not 2 and can't be prime.

n odd

We begin by completing the square

$$\begin{aligned} n^4 + 4^n &= n^4 + 4^n \\ &= \left(n^2\right)^2 + \left(2^n\right)^2 \\ &= \left(n^2 + 2^n\right)^2 - 2n^2 2^n \end{aligned}$$

We from here we observe that $2^n 2 = 2^{n+1}$, since n is odd $n+1$ is even yielding $2^{n+1} = 2^{2k}$. We can see we have a difference of squares

$$\begin{aligned} \left(n^2 + 2^n\right)^2 - 2n^2 2^n &= \left(n^2 + 2^n\right)^2 - \left(2^n n\right)^2 \\ &= \left(n^2 + 2^n + 2^n n\right)\left(n^2 + 2^n - 2^n n\right) \end{aligned}$$

since we are restricted to $n > 1$ we can see that both $(n^2 + 2^n + 2^n n) > 1$ and $(n^2 + 2^n - 2^n n) > 1$ for all n. Making $n^4 + 4^n$ composite as desired.

13. Let a, b, c be positive integers, and let $d = (a, b)$. Since $d|a$, there exists an integer h with $a = dh$. Show that $a|bc$, then $h|c$.

Joe Starr

We will proceed with a transitive proof:

$$\begin{aligned} a|abc &\rightarrow a|(a, b)\, c \\ &\rightarrow a|dc \\ &\rightarrow dh|dc \\ &\rightarrow h|c \end{aligned}$$

14. Show that $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]$.

Joe Starr

Let $x \in (a\mathbb{Z} \cap b\mathbb{Z})$, since $x \in a\mathbb{Z}$ we have $x = aq_1$, similarly since $x \in b\mathbb{Z}$ we have$x = bq_2$. We can see that $x = abq$, this means x is a multiple of $[a, b]$ putting $x \in [a, b]$. Next, we let $x \in [a, b]\,\mathbb{Z}$, this means x is of the form $x = [a, b]\,q$. We can see that $a|x$ and $b|x$ since $a|[a, b]$, This makes $x \in a\mathbb{Z}$ and $x \in b\mathbb{Z}$, as desired.

17. Let a, b be nonzero integers. Prove $(a, b) = 1$ if and only if $(a + b, ab) = 1$.

Joe Starr

$\Rightarrow$ We let $(a, b) = 1$, then consider the $(a + b, ab)$. We assume $(a + b, ab) = d$, with $d > 1$. Since $d > 1$ there must exist p a prime such that $p|d$. This means that $p|a + b$ and $p|ab$. Consequently, either $p|a$ or $p|b$. WOLG we have $p|a$, and since $p|a + b$ it must be that $p|b$. Finally, since $p|a$ and $p|b$, $p|(a, b)$ a contradiction. So $(a + b, ab) = 1$.

$\Leftarrow$ We let $(a + b, ab) = 1$, then consider the (a, b). We assume $(a, b) = d$, with $d > 1$. Since $d > 1$ there must exist p a prime such that $p|d$. This means that $p|a$ and $p|b$, further $p|ab$. Since p divides a and b, we have $p|a + b$. Finally, since $p|ab$, and $p|a + b$, $p|(a + b, ab)$, a contradiction so $(a, b) = 1$.

18. Let a, b be nonzero integers with $(a, b) = 1$. Compute $(a + b, a - b)$.

Joe Starr

We know that $d = (a + b, a - b)$, this means that $d|a+b$ and $d|a-b$. From here we have that $d|(a + b) + (a - b) \to d|2a$ and $d|(a + b) - (a - b) \to d|2b$. Since d divides both $2a$ and $2b$, d must also divide $2\,(a, b)$. Since $(a, b) = 1$ we have $(a + b, a - b) = 2$.

19. Let a and b be positive integers, and let m be an integer such that $ab = m\,(a, b)$. Without using the prime factorization theorem, prove that $(a, b)\,[a, b] = ab$ by verifying that m satisfies the necessary properties of $[a, b]$.

Joe Starr

We let $d = (a, b)$, this means that $ab = md$. We first show $a|m$ and $b|m$,

$$\begin{aligned} ab = md &\rightarrow a\,(dq) = md \\ &\rightarrow adq - md = 0 \\ &\rightarrow d(aq - m) = 0 && (by def d > 0) \\ &\rightarrow aq = m \\ &\rightarrow a|m \end{aligned}$$

similarly for b.

Next we will show that if $a|c$ and $b|c$ then $m|c$. We have that $c = aq_1 = bq_2$ or $c^2 = abq$. We can multiply $ab = md$ by q giving $abq = mdq$, this means we have $c^2 = mdq$, which is true only if $c = mdq$, $m|c$ as desired.

20. A positive integer a is called a square if $a = n^2$ for some $n \in \mathbb{Z}$. Show that the integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

Joe Starr

Let $a \in \mathbb{Z}$ be a square. Since a is a square by definiton there exists a n such that $nn = a$. Now by the fundamental theorem of arithmetic we know n has a prime factorization,written $p_1^{n_1} \cdots p_k^{n_k}$. If we consider nn, we have $nn = \left(p_1^{n_1} \cdots p_k^{n_k}\right)\left(p_1^{n_1} \cdots p_k^{n_k}\right)$, by combining terms we can see that $nn = \left(p_1^{2n_1} \cdots p_k^{2n_k}\right)$, as desired.

23. Let p and q be prime numbers. Prove that $pq + 1$ is a square if and only if p and q are twin primes.

Joe Starr

We begin by letting selecting p a prime and q a prime such that $q = p + 2$. Now we consider pq,

$$pq \to p\,(p+2)$$
$$\to p^2 + p2$$

We now consider $p + 1$, if we take $(p+1)^2$, we get $p^2 + 2p + 1$. It's obvious that $pq + 1 = p^2 + p2 + 1 = (p+1)^2$, so $pq + 1$ is a square when p and q are twin primes. We can now consider p a prime, and q a prime such that $q = p + n$ with $n > 2$. If we calculate pq we see that,

$$pq \to p\,(p+n)$$
$$\to p^2 + pn$$

we then have that $pq + 1 = p^2 + pn + 1$ with $n > 2$, this is not a square, showing when p and q aren't twin primes $pq + 1$ is not a square.

26. Prove that if $a > 1$, then there is a prime p with $a < p \leq a! + 1$.

Joe Starr

We observe that $a! + 1$ is either prime or composite, if $a! + 1$ is prime we are done, if $a! + 1$ is composite we know by the fundamental theorem of arithmetic that $a! + 1$ has prime factors. Now if all prime factors p are such that $p \leq a$ since $p|a!$ we see that if we divide $a! + 1$ by any of these we get a remainder of 1, a contradiction so there must be a prime factor p with $a < p$.

Note: this is basically the same argument as euclid's proof of infinite primes

29. Show that $\log 2/\log 3$ is not a rational number.

Joe Starr

We observe this is an application of the change of base formula, making $\frac{\log 2}{\log 3} = \log_3 2$.

From here we have $x = \log_3 2 \rightarrow 3^x = 2$, if x is rational then there exist m and n such that $\frac{m}{n} = x$. We now have $3^{\frac{m}{n}} = 2 \rightarrow 3^m = 2^n$, a contradiction since there is no m and n that satisfy this equivalence, making $\log 2/\log 3$ irrational as desired.

CHAPTER 2 SECTION

I <3 my Wayne State Libraries! Do you?

2.1 A Subsection

CHAPTER 3 SECTION

I <3 my Wayne State Libraries! Do you?

3.1 A Subsection

CHAPTER 4 SECTION

I <3 my Wayne State Libraries! Do you?

4.1 A Subsection

I <3 my Wayne State Libraries! Do you?

5.1 A Subsection

CHAPTER 6 SECTION

I <3 my Wayne State Libraries! Do you?

6.1 A Subsection

CHAPTER 7 SECTION

I <3 my Wayne State Libraries! Do you?

7.1 A Subsection

CHAPTER 8 SECTION

I <3 my Wayne State Libraries! Do you?

8.1 A Subsection

CHAPTER 9 SECTION

I <3 my Wayne State Libraries! Do you?

9.1 A Subsection

CHAPTER 10 SECTION

I <3 my Wayne State Libraries! Do you?

10.1 A Subsection