Number Theory Homework.

1. The greatest common divisor and Bezout's Theorem

Definition 1. If a and b are integers, not both zero, then c is a ***common divisor*** of a and b iff $c \mid a$ and $c \mid b$.

More generally if $a_1, a_2, \ldots, a_n$ are integers not all zero, then c is a ***common divisor*** of $a_1, a_2, \ldots, a_n$ iff $c \mid a_j$ for all $j = 1, 2, \ldots, n$. □

As an example, the divisors of 48 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12, \pm16, \pm24, \pm48$. The divisors of 60 are $\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm10, \pm12, \pm15, \pm20, \pm30, \pm60$. Therefore the common divisors of 48 and 60 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$.

Definition 2. If a and b are integers, not both zero, then d is the ***greatest common divisor*** of a and b iff d is a common divisor of a and b and if c is any other common divisor of a and b, then $c \leq d$. We use the notation $d = \gcd(a, b)$.

This extends to more than two numbers. If $a_1, a_2, \ldots, a_n$ are integers, not all zero, then d is the ***greatest common divisor*** of $a_1, a_2, \ldots, a_n$ iff d is a common divisor of $a_1, a_2, \ldots, a_n$ iff d and $c \leq d$ for any other common divisor of c of the numbers. In this case we write $d = \gcd(a_1, a_2, \ldots, a_n)$ □

From our list of the common divisors of 48 and 60 we see the largest one is 12 and therefore $\gcd(48, 60) = 12$.

Any integer other than 0 has only a finite number of divisors and so any collection of integers not all zero will only have a finite number of common factors. The maximum of any finite number of integers always exists. Thus the greatest common divisor always exists and is a positive number.

Definition 3. The integers a and b are ***relatively prime*** iff $\gcd(a, b) = 1$. More generally, the integers $a_1, a_2, \ldots, a_n$ are ***relatively prime*** iff $\gcd(a_1, a_2, \ldots, a_n) = 1$. □

Problem 1. Here are a couple of problems related to basic properties of the gcd.

(a) If p is prime and $p \nmid a$, the $\gcd(a, p) = 1$.
(b) If $\gcd(a, b) = d$ and $c > 0$, then $\gcd(ac, bc) = cd$.
(c) Give an example of three positive integers a, b, c with $\gcd(a, b) > 1$, $\gcd(a, c) > 1$, $\gcd(b, c) > 1$, but $\gcd(a, b, c) = 1$. That is find three relatively prime integers , but such that no pair of them are relatively prime. □

Here is anther basic property.

Proposition 4. *If a and b are not both zero, then for any integers x and y*

$$\gcd(a, b) \mid (ax + by).$$

Problem 2. Prove this. □

Here is a basic result, which also make computing the greatest common divisor of a pair of large integers easier than you might think.

Proposition 5. *For any pair of integers a and b with $a \neq 0$ and any integer k*

$$\gcd(a, b) = \gcd(a, b + ka).$$

In particular if $a > 0$ and $b = qa + r$ with $0 \leq r < a$, then

$$\gcd(a, b) = \gcd(a, r).$$

Problem 3. Prove this. *Hint:* From $\gcd(a, b) \mid (a + kb)$ (explain why his holds) we see $gcd(a, b) \mid \gcd(a, b + ka)$. But $b = (b + ka) + (-k)a$ so by the same argument (with b replaced by $b + ka$ and k by $-k$) we also have $\gcd(a, b + ka) \mid \gcd(a, b)$. □

Hare are examples of how this can be used to compute greatest common divisors. To start with a short one

$$\begin{aligned}
\gcd(25, 65) &= \gcd(25, 2 \cdot 25 + 10) \\
&= \gcd(25, 10) \\
&= \gcd(10, 25) \\
&= \gcd(10, 2 \cdot 10 + 5) \\
&= \gcd(10, 5) \\
&= \gcd(5, 2 \cdot 5 + 0) \\
&= \gcd(5, 0) \\
&= 5
\end{aligned}$$

and here is one that is not easily done by factoring.

$$\begin{aligned}
\gcd(632, 2642) &= \gcd(632, 4 \cdot 632 + 114) \\
&= \gcd(632, 114) \\
&= \gcd(114, 632) \\
&= \gcd(114, 5 \cdot 114 + 62) \\
&= \gcd(62, 114) \\
&= \gcd(62, 1 \cdot 62 + 52) \\
&= \gcd(52, 62) \\
&= \gcd(52, 1 \cdot 52 + 10) \\
&= \gcd(10, 52) \\
&= \gcd(10, 5 \cdot 10 + 2) \\
&= \gcd(2, 10) \\
&= 2.
\end{aligned}$$

After you have done a few of these you start just writing down the remainder. Thus the last example could be shortened to

$$\begin{aligned}
\gcd(632, 2642) &= \gcd(114, 632) && (r = 114 \text{ when } 632 \text{ is divided into } 2642)\\
&= \gcd(62, 114) && (r = 62 \text{ when } 114 \text{ is divided into } 632)\\
&= \gcd(52, 62) && (r = 52 \text{ when } 62 \text{ is divided into } 114)\\
&= \gcd(10, 52) && (r = 10 \text{ when } 52 \text{ is divided into } 62)\\
&= \gcd(2, 10) && (r = 2 \text{ when } 10 \text{ is divided into } 52)\\
&= \gcd(0, 2) && (r = 0 \text{ when } 2 \text{ is divided into } 10)\\
&= 2
\end{aligned}$$

where you would most likely not write down the comments about $r = 144$ etc.

Problem 4. Use this method (called the ***Euclidean algorithm***) to find the following greatest common divisors. We shall study this algorithm in much more detail later in the term.

$$\gcd(64, 81),\ \gcd(6, 121),\ \gcd(169, 273),\ \gcd(51, 187),\ \gcd(999, 2187).$$ □

The following is maybe the most important elementary fact about greatest common divisors and relatively prime integers.

Theorem 6 (Bezout's Theorem)**.** *If a and b are integers, not both zero, then there are integers x and y such that*

$$ax + by = \gcd(a, b).$$

In particular if a and b are relatively prime, there are integers x, y such that $ax + by = 1$.

Remark 7. The proof here is based on the fact that all ideals are principle and shows how ideals are useful. This proof is short, but is somewhat unsatisfying as it does give a method for finding integers x and y. Later we will give anther proof, based on the Euclidean algorithm, which is constrictive in that it gives an algorithm for finding x and y. □

Problem 5. Prove Theorem 6 along the following lines. Set

$$I = \{ax + by : x, y \in Z\}.$$

We have already seen that this is an ideal. We have also shown that all ideals are principal. That is there is a d such that

$$I = I_d = \{zd : z \in \mathbb{Z}\}.$$

Note that $I_{-d} = I_d$, so by possibly replacing d by $-d$ we assume that $d > 0$.

(a) Explain why $d \mid a$ and $d \mid b$ and therefore d is a common divisor of a and b. *Hint:* Show that $a, b \in I$. Then use $I = I_d$.
(b) Explain why $\gcd(a, b) \mid d$. *Hint:* Proposition 4.
(c) Now show $d = \gcd(a, b)$.

(d) Finish the proof by explaining why there are integers x and y with $\gcd(a, b) = d = ax + by$. □

Corollary 8. *If c is a common divisor of a and b, then*

$$c \mid \gcd(a, b).$$

Problem 6. Prove this. *Hint:* Combine Theorem 6 with Proposition 4.

Theorem 9. *If $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.*

Problem 7. Prove this. *Hint:* This is one of many times in the near future we will be using the assumption $\gcd(a, b) = 1$ by using that there are integers x and y with $ax+bx = 1$. As we have $a \mid bc$ there is a integer k such $bc = ak$. Multiply $ax + bx = 1$ by c to get $acx + bcx = c$. Now replace bc by ak and the result is $acx + akx = c$. Now it should be easy to show $a \mid c$. □

The following is really a corollary to the last result, but is important enough to get promoted to a Proposition.

Proposition 10. *If p is prime and $p \mid ab$, then $p \mid a$ or $p|b$. That is if a prime divides a product, then it divides one of the factors.*

Proof. If $p \mid a$, then we are done. So assume $\nmid a$. As the only positive factors of p are p and 1, we have that either $\gcd(p, a) = p$, or $\gcd(p, a) = 1$. As $p \nmid a$, we have $\gcd(p, a) = 1$. Then $p \mid b$ by the last Theorem. □

Problem 8. This is to show that it is important that p is prime in the last result. Give examples of

(a) Positive integers a and b such that $6 \mid ab$, but $6 \nmid a$ and $6 \nmid b$.
(b) Positive integers a and b such that $35 \mid ab$, but $35 \nmid a$ and $35 \nmid b$.
(c) Positive integers a and b such that $9 \mid ab$, but $9 \nmid a$ and $9 \nmid b$.

Corollary 11. *If p is a prime and p divides a product of several integers, then it divides one of the factors. That is if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_j$ for some j.*

Problem 9. Use induction to prove this from Proposition 10. □

Lemma 12. *If a and b are integers such that there are integers x and y with $ax + by = 1$, then $\gcd(a, b) = 1$.*

Proof. By Proposition 4 we have that $\gcd(a, b)|1$, which implies $\gcd(a, b) = 1$. □

Proposition 13. *If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$. That is if a number is relatively prime to two numbers, then it is relatively prime to their product.*

Problem 10. Prove this. *Hint:* (This is a good example of the fact that in 87.5% of the proofs we will have involving the hypothesis $\gcd(a, b) = 1$, the way this will be used to to use that that are integers x and y with $ax + by = 1$.) As $\gcd(a, b) = 1$, Bézout's Theorem gives us integers x and

y such that $ax + by = 1$. Likewise there are integers x' and y' such that $ax' + cy' = 1$. Thus

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (ax + by)(ax' + cy') \\ &= a^2xx' + acxy' + abyx' + bcx'y' \\ &= a(axx' + cxy + byx) + b(cx'y') \\ &= ax'' + by'' \end{aligned}$$

where $x'' = (axx' + cxy + byx)$ and $y'' = cx'y'$ are integers. Now Lemma 12 should tell you something. □

Corollary 14. *If $b_1, b_2, \ldots, b_n$ are all relatively prime to a then the product $b_1b_2 \cdots b_n$ is also relatively prime to a. (Letting $b_1 = b_2 = \cdots = b_n = b$ this yields that if $\gcd(a, b) = 1$, then $\gcd(a, b^n) = 1$.)*

Problem 11. Use induction to prove this. □

A variant on this is

Proposition 15. *If $\gcd(a, b) = 1$ then for any positive integers m, n we have $\gcd(a^m, b^n) = 1$.*

Problem 12. Prove this. *Hint:* By the last corollary, $\gcd(a, b^n)$. But we know that if $\gcd(A, B) = 1$, then $\gcd(A, B^m) = 1$. Think about letting $A = b^n$ and $B = a$. □

Proposition 16. *If a and b are not both zero, then*

$$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1.$$

Problem 13. Prove this. *Hint:* Let $d = \gcd(a, b)$ and set

$$a' = \frac{a}{d} \qquad \text{and} \qquad b' = \frac{b}{d}.$$

Then $a = a'd$ and $b = b'd$ and our goal is to prove $\gcd(a', b') = 1$. By Bézout's Theorem there are integers x and y such that

$$ax + by = d.$$

Then using $a = a'd$ and $b = b'd$ in this equation, along with with Lemma 12 should do the trick. □

Problem 14. Define the ***Fermat numbers***[1] to be the integers

$$F_n = 2^{2^n} + 1.$$

[1]Fermat conjectured these were all prime. The first several, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, are prime, but the next one is composite $F_5 = 641 \cdot 6700417$. Currently it is known F_n is composite for $5 \leq n \leq 32$. It is unknown if any of the F_n are prime for $n \geq 5$. It is known $F_{3,329,780}$ is composite.

(a) Use induction to show

$$F_0F_1F_2\cdots F_{n-1} = F_n - 2.$$

(b) Use part (a) to show if $m \neq n$ then $\gcd(F_m, F_n) = 1$. *Hint:* Assume $m < n$. If c is a common factor of F_m and F_n then it is a common factor of $F_n - F_1F_2\cdots F_{n-1} = 2$.

(c) Use part (b) to give anther proof there are infinitely primes. *Hint:* If p and q are primes with $p \mid F_m$, $q \mid F_n$, and $m \neq n$, show $p \neq q$.

These results are from a letter of Christian Goldbach to Leonhard Euler written in 1730. □

1.1. **The least common multiple.** Closely related to the greatest common divisor is the least common multiple.

Definition 17. If a and b are integers then m is a ***common multiple*** of a and b iff $a \mid m$ and $b \mid m$. The positive integer ℓ is the ***least common multiple*** of a and b iff it is a common multiple of a and b and for any other positive common multiple, m, of a and b we have $\ell \leq m$. We denote the least common multiple of a and b by $\operatorname{lcm}(a, b)$. □

For example

$$\operatorname{lcm}(15, 12) = 60,\ \operatorname{lcm}(-19, 5) = 90,\ \operatorname{lcm}(2^4{\cdot}5^2{\cdot}7, 2{\cdot}3^7{\cdot}5{\cdot}11^3) = 2^4{\cdot}3^7{\cdot}5^2{\cdot}7{\cdot}11^3.$$

Proposition 18. *If a, b, c are positive integers, then* $\operatorname{lcm}(ac, bc) = c\operatorname{lcm}(a, b)$.

Problem 15. Prove this. □

Lemma 19. *If a and b are positive integers, and $\gcd(a, b) = 1$, then $\operatorname{lcm}(a, b) = ab$.*

Problem 16. Prove this. *Hint:* As a start because $b \mid \operatorname{lcm}(a, b)$ there is an integer k such that $\operatorname{lcm}(a, b) = bk$. Also $a \mid \operatorname{lcm}(a, b) = bk$. Now use Theorem 9 to deduce $a \mid k$. □

Theorem 20. *If a and b are positive integers, then*

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

This is often written as

$$\gcd(a, b)\operatorname{lcm}(a, b) = ab.$$

Problem 17. Prove this. *Hint:* Let $d = \gcd(a, b)$. Then there are integers a' and b' such that $a = a'd$ and $b = b'd$.

(a) Show $\gcd(a', b') = 1$.

(b) Let m be a common multiple of both a and b, that is $a \mid m$ and $b \mid m$. Then there is an integer k such that $m = ak = a'dk$.

(c) Use $b'd = b \mid m = a'dk$ to show $b' \mid a'k$.

(d) Use $\gcd(a', b') = 1$ and $b' \mid a'k$ to conclude there is an integer ℓ such that $k = b'\ell$.

(e) Put these pieces together to see $m = a'b'd\ell$. As m was any common multiple of a and b explain why this shows $\text{lcm}(a, b) = a'b'd$ and that this finishes the proof. □

Problem 18. Use the last proposition and the Euclidean algorithm of Problem 4 to find the following.

$$\text{lcm}(423, 801), \qquad \text{lcm}(354, 192), \qquad \text{lcm}(79, 129)$$

□

1.2. **The Fundamental Theorem of Arithmetic.** We now show that factorization into primes is essentially unique. This seems to have first been explicitly stated by Gauss in his book *Disquisitiones Arithmeticae* published in 1798. But it was being used implicitly for many years before then.

Theorem 21 (Fundamental Theorem of Arithmetic)**.** *Let $a \geq 2$ be a positive integers be an integer. Then a can be factored into primes in a unique way. Explicitly by uniqueness we mean if*

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

with all of $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_n$ prime, then $m = n$ and after reordering $p_j = q_j$ for $j = 1, 2, \ldots, n$.

Problem 19. Prove this. *Hint:* We have seen in an earlier homework set that a is a product of primes. So we only have to prove uniqueness.

One standard proof uses induction on m. If $m = 1$, then $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ reduces to $p_1 = q_1 q_2 \cdots q_n$. If $n \geq 2$, this would imply that p_1 is composite, a contradiction. Therefore $n = 1$ and we have $p_1 = q_1$. This is the base case.

The induction hypothesis is that the result is true for for m. Assume $p_1 p_2 \cdots p_{m+1} = q_1 q_2 \cdots q_{n+1}$ as in the statement of the theorem and proceed as follows

(a) Explain why $p_{m+1} \mid q_1 q_2 \cdots q_{n+1}$.
(b) Use Proposition 11 to show that $p_{m+1} \mid q_j$ for some j. By possibly reordering $q_1, q_2, \ldots, q_{n+1}$ we assume $p_{m+1} \mid q_{n+1}$.
(c) Show $p_{m+1} = q_{n+1}$.
(d) Use the last step to show

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

(e) Use the induction hypothesis to complete the proof. □

The ***standard factorization*** of an integer is

$$a = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$$

where $p_1, \ldots, p_\ell$ are the primes dividing a listed in increasing order. For example:

$$5 = 5, \quad 24 = 2^2 \cdot 3, \quad 360 = 2^3 \cdot 3^2 \cdot 5, \quad 4158002 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11.$$

and Table 1 gives the standard factorization of the first one hundred numbers natural numbers.

n	Factors	n	Factors	n	Factors	n	Factors	n	Factors
1	1	21	$3 \cdot 7$	41	41	61	61	81	3^4
2	2	22	$2 \cdot 11$	42	$2 \cdot 3 \cdot 7$	62	$2 \cdot 31$	82	$2 \cdot 41$
3	3	23	23	43	43	63	$3^2 \cdot 7$	83	83
4	2^2	24	$2^3 \cdot 3$	44	$2^2 \cdot 11$	64	2^6	84	$2^2 \cdot 3 \cdot 7$
5	5	25	5^2	45	$3^2 \cdot 5$	65	$5 \cdot 13$	85	$5 \cdot 17$
6	$2 \cdot 3$	26	$2 \cdot 13$	46	$2 \cdot 23$	66	$2 \cdot 3 \cdot 11$	86	$2 \cdot 43$
7	7	27	3^3	47	47	67	67	87	$3 \cdot 29$
8	2^3	28	$2^2 \cdot 7$	48	$2^4 \cdot 3$	68	$2^2 \cdot 17$	88	$2^3 \cdot 11$
9	3^2	29	29	49	7^2	69	$3 \cdot 23$	89	89
10	$2 \cdot 5$	30	$2 \cdot 3 \cdot 5$	50	$2 \cdot 5^2$	70	$2 \cdot 5 \cdot 7$	90	$2 \cdot 3^2 \cdot 5$
11	11	31	31	51	$3 \cdot 17$	71	71	91	$7 \cdot 13$
12	$2^2 \cdot 3$	32	2^5	52	$2^2 \cdot 13$	72	$2^3 \cdot 3^2$	92	$2^2 \cdot 23$
13	13	33	$3 \cdot 11$	53	53	73	73	93	$3 \cdot 31$
14	$2 \cdot 7$	34	$2 \cdot 17$	54	$2 \cdot 3^3$	74	$2 \cdot 37$	94	$2 \cdot 47$
15	$3 \cdot 5$	35	$5 \cdot 7$	55	$5 \cdot 11$	75	$3 \cdot 5^2$	95	$5 \cdot 19$
16	2^4	36	$2^2 \cdot 3^2$	56	$2^3 \cdot 7$	76	$2^2 \cdot 19$	96	$2^5 \cdot 3$
17	17	37	37	57	$3 \cdot 19$	77	$7 \cdot 11$	97	97
18	$2 \cdot 3^2$	38	$2 \cdot 19$	58	$2 \cdot 29$	78	$2 \cdot 3 \cdot 13$	98	$2 \cdot 7^2$
19	19	39	$3 \cdot 13$	59	59	79	79	99	$3^2 \cdot 11$
20	$2^2 \cdot 5$	40	$2^3 \cdot 5$	60	$2^2 \cdot 3 \cdot 5$	80	$2^4 \cdot 5$	100	$2^2 \cdot 5^2$

TABLE 1. Prime factorization of natural numbers up to 100.

If we know the prime factorization of two integers a and b, then it is easy to compute their greatest common divisor. For example if $p_1, \ldots, p_n$ is a list of all the primes that divide either a or b, then

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where the α_j's and β_j are non-negative integers. (If a prime p_j divides a but not b then $\beta_j = 0$ and likewise $\alpha_j = 0$ if p_j divides b but not a.) In product notation this is

$$a = \prod_{j=1}^{n} p_j^{\alpha_j}, \qquad b = \prod_{j=1}^{n} p_j^{\beta_j}.$$

Then

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_n^{\min(\alpha_n, \beta_n)} = \prod_{j=1}^{n} p_j^{\min(\alpha_j, \beta_j)}.$$

For example if

$$a = 2^4 \cdot 5^3 \cdot 11^5 \cdot 37^4 \cdot 41, \qquad b = 5^4 \cdot 11^7 \cdot 37$$

then

$$\gcd(a, b) = 2^0 \cdot 5^3 \cdot 11^5 \cdot 37^1 \cdot 41^0 = 5^3 \cdot 11^5 \cdot 37.$$

Proposition 22. *Every positive integer n can be uniquely written as a power of two times an odd number. (Here the power of 2 can be $2^0 = 1$.) That is every $n \geq 1$ can be uniquely written as $n = 2^k m$ where $k \geq 0$ and m is odd. The number m is the* ***odd part*** *of n.*

Problem 20. Use the Fundamental Theorem of Arithmetic to prove this. □

Remark 23. Now that we have the Fundamental Theorem of Arithmetic, we can revisit some results we have proven by other methods. For example it is not hard to see that for positive integers a and b that $\gcd(a, b) = 1$, that is a and b are relatively prime, if and only if a and b have no prime factors in common. But for any positive integer m the numbers a and a^n have the same prime factors (they just appear to higher powers in a^m). Likewise b^n and b have the same prime factors. Thus if a and b have no prime factors in common, then neither do a^m and b^n. That is that is $\gcd(a, b) = 1$ implies $\gcd(a^m, b^n) = 1$. Thus we have given anther proof of Proposition 15.

Likewise assume that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Then a and b have no prime factors in common and a and c have no prime factors in common. The prime factors of bc are just the union of the prime factors of b and c (or put differently any prime factor of bc is a prime factor of b or a prime factor of c). Thus no prime factor of bc is a factor of a. Therefore $\gcd(a, bc) = 1$ and we have given anther proof of Proposition 13. □

1.3. **The rational root test and showing some square and higher roots of integers are irrational.** We recall a rational number is one of the form a/b where a and b are integers and $b \neq 0$. It is ***lowest terms***, (also called ***reduced form***) iff $\gcd(a, b) = 1$. If $r = a/b$ is any rational number, then let $d = \gcd(a, b)$. Write $a = a'd$ and $b = b'd$ where $a' = a/d$ and $b' = b/d$. Then by Proposition 16 we have $\gcd(a', b') = 1$. Thus

$$\frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'}.$$

This shows every rational number can be put in reduced form.

We also recall that a ***polynomial*** is a function of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots, a_n$ are the coefficients of $p(x)$ and are assumed to be real numbers. If $a_n \neq 0$ then the ***degree*** of $f(x)$ is n. The number r is a ***root*** (or ***zero***) of $f(x)$ iff $f(r) = 0$.

The following well known result goes back to Descartes and is a nice application of our results to date about relatively prime numbers.

Theorem 24. *Let $f(x)$ be a polynomial with integer coefficients:*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

If $r = p/q$ is a rational number in reduced form that is a root of $p(x)$. Then

$$p \mid a_0 \qquad \text{and} \qquad q \mid a_n.$$

Problem 21. Prove this along the following lines:

(a) As $r = p/q$ is a root of $f(x)$ we have $f(p/q) = 0$. Clear this of fractions to get

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

(b) Rewrite this as

$$a_n p^n = -q \left(p^{n-1} + a_{n-2} p^{n-2} q + \cdots + a_1 p q^{n-2} + a_0 q^{n-1} \right)$$

to conclude $q \mid a_n p^n$. Now use Proposition 15 and Theorem 9 to conclude $q \mid a_n$.

(c) Do a similar calculation to show $p \mid a_0$. □

While this is useful in finding rational roots of polynomials, it is also gives an easy way to show that certain numbers are irrational.

Definition 25. A real number is ***irrational*** iff it is not a rational number. □

It takes a little work to produce any irrational numbers. The first explicit example seems to have been $\sqrt{2}$ which has shown to be irrational by someone (possibly Hippasus of Metapontum) in Greece about the 5th century BC. (It is possible the irrationality of $\sqrt{2}$ was known even earlier in India. See the Wikipedia article *Irrational number* for more information.)

Proposition 26. *The number $\sqrt{2}$ is irrational.*

Proof. Let $f(x) = x^2 - 2$. This is a polynomial with integer coefficients and

$$f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 2 - 2 = 0$$

and therefore $\sqrt{2}$ is a root of $f(x)$. By the Rational Root Test the only possible rational roots of $f(x) = x^2 - 2$ are of the form $r = p/q$ where $p \mid 2$ and $q \mid 1$. Thus $q = \pm 1$ and $p = \pm 1, \pm 2$, which gives the possible rational roots as

$$r = \pm 1 \qquad \text{or} \qquad r = \pm 2.$$

However

$$f(\pm 1) = (\pm 1)^2 - 2 = -1 \neq 0, \qquad f(\pm 2) = (\pm 2)^2 - 2 = 2 \neq 0.$$

As these are only possible rational roots, we conclude that $f(x) = 0$ has no rational roots. But $\sqrt{2}$ is a root, so it is not a rational number. □

This argument generalizes to shows the square roots of positive integers that are not perfect squares are irrational.

Proposition 27. *If n is a positive integer that is not the square of any integer. Then $\sqrt{n}$ is irrational. (Put a little differently, if n is a positive integer, then either $\sqrt{n}$ is an integer, or it is irrational.)*

Proof. The number $\sqrt{n}$ is a root of the polynomial $f(x) = x^2 - n$. By the rational root test, the only rational roots are of the form $r = p/q$ where $q \mid 1$. The only divisors of 1 are ± 1, thus the only possible rational roots of $x^2 - n$ are $r = p/(\pm 1) = \pm p$. That is the only possible rational roots of $f(x) = x^2 - n$ are integers. But our hypothesis on n is that it is not a perfect square, so $f(x)$ has no rational roots. Therefore $\sqrt{n}$ is irrational. □

More generally

Proposition 28. *If $m \geq 2$ is an integer and n is a positive integer that is not the m-th power of an integer, then $\sqrt[m]{n}$ is irrational. (That is if $\sqrt[m]{n}$ is not an integer, then it is irrational.)*

Problem 22. Prove this. □

Problem 23. Here we give some basic properties of rational and irrational numbers.

(a) If a and b are rational then so are $a + b$, $a - b$, ab, a/b (where $b \neq 0$ in the last case).
(b) If a is rational and b is irrational, then $a + b$ is irrational. If $b \neq 0$, then ab is irrational.
(c) Given an example where a and b are both irrational and $a+b$ is irrational.
(d) Given an example where a and b are both irrational and $a+b$ is rational.
(e) Given an example where a and b are both irrational and ab is irrational.
(f) Given an example where a and b are both irrational and ab is rational.

□

In light of the last problem, it is not clear immediately if $\sqrt{2} + \sqrt{3}$ is rational or irrational. We will show that it is irrational by showing that it is the root of a polynomial with integer coefficients and using the rational roots test. To start let

$$\alpha = \sqrt{2} + \sqrt{3}.$$

Then

$$\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}.$$

Rearrange and square to get

$$(\alpha^2 - 5)^2 = (2\sqrt{6})^2 = 24.$$

Therefore

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

This shows α is a root of $f(x) = x^4 - 10x^2 + 1$. The rational root test yields that the only possible rational roots of $f(x)$ are ± 1. But $f(\pm 1) = (\pm 1)^4 - 10(\pm 1)^2 + 1 = -8 \neq 0$, and therefore $f(x)$ has no rational roots. Thus $\alpha = \sqrt{2} + \sqrt{3}$ is irrational. (A shorter, and possibly more natural proof, would be to assume that α is rational. Then $(\alpha^2 - 5)/2 = \sqrt{6}$ would be rational, contradicting Proposition 27.)

While this method is good for showing that roots of integers an some closely related numbers are irrational, it quickly gets complicated. For example consider the number

$$\beta = \sqrt{2} + \sqrt{3} + \sqrt{5}.$$

We would like to believe, and it is true, this is irrational. This can be shown by the rational root test. First you work very hard and show β is a root of the polynomial[2]

$$f(x) = x^8 - 40x^6 + 352x^4 - 960x^2 + 576.$$

By the rational root test any rational root of this is an integer and a factor of $576 = 2^6 \cdot 3^2$. This has 21 positive factors and if you test all of them you do find that β is irrational. There are proofs which are more transparent and less computational based on ideas from abstract algebra. If you take an algebra class where you study field theory and Galois Theory you will see these proofs.

1.4. **Some well known numbers that are irrational.** This is a bit of an aside, but because it came up in class and because it is interesting, here are proofs that well e and π are irrational. Recall that one way to compute the number e is with the series

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \frac{1}{6!} + \cdots$$

We will need anther calculus fact:

Proposition 29. *If $|r| < 1$ then*

$$\sum_{k=0}^{\infty} ar^k = a + ar + ar^2 + ar^3 + \cdots = \frac{a}{1-r}.$$

Proof. One of the formulas we proved in the first week of class was that for $r \neq 1$

$$a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a - ar^{n+1}}{1-r}.$$

If $|r| < 1$ then $\lim_{n\to\infty} ar^{n+1} = 0$. So the result follows by letting letting $n \to \infty$ in the last displayed formula. □

Theorem 30. *The number e is irrational.*

Problem 24. Prove this along the following lines (This argument seems to be due to Euler). Assume, towards a contradiction, that e is rational, say $e = p/q$.

$$\frac{p}{q} = e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{(q-1)!} + \frac{1}{q!} + \cdots$$

[2]I did this with the computer package Sage which is an open source alternative to the commercial software packages Maple and Mathematica. Sage can be down loaded for free.

Multiply this by $q!$ to get

$$\begin{aligned} q!\frac{p}{q} &= q!\left(1+1+\frac{1}{2!}+\cdots+\frac{1}{(q-1)!}+\frac{1}{q!}+\frac{1}{(q+1)!}+\cdots\right) \\ &= \left(q!+q!+\frac{q!}{2!}+\cdots+\frac{q!}{(q-1)!}+\frac{q!}{q!}\right) \\ &\qquad +\left(\frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\frac{q!}{(q+3)!}+\cdots\right) \end{aligned}$$

(a) Explain why

$$N_1 = q!\frac{p}{q}$$

is an integer.

(b) Explain why

$$N_2 = q!+q!+\frac{q!}{2!}+\cdots+\frac{q!}{(q-1)!}+\frac{q!}{q!}$$

is an integer. We thus have

$$N_1 = N_2 + \rho$$

where N_1 and N_2 are integers and

$$\rho = \frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\frac{q!}{(q+3)!}+\cdots.$$

(c) Justify the following steps

$$\begin{aligned} \rho &= \frac{q!}{(q+1)!}+\frac{q!}{(q+2)!}+\frac{q!}{(q+3)!}+\cdots \\ &= \frac{1}{(q+1)}+\frac{1}{(q+1)(q+2)}+\frac{1}{(q+1)(q+2)(q+3)}+\cdots \\ &< \frac{1}{(q+1)}+\frac{1}{(q+1)^2}+\frac{1}{(q+1)^3}+\frac{1}{(q+1)^4}+\cdots \\ &= \frac{\dfrac{1}{(q+1)}}{1-\dfrac{1}{(q+1)}} \\ &= \frac{1}{q} \\ &\leq 1. \end{aligned}$$

Thus $\rho < 1$.

(d) Finish by showing $N_1 = N_2 + \rho$ and $0 < \rho < 1$ together yield a contradiction. □

We can do better. However the proof, while not using anything particularly advance, is very clever and I do not know any way to motivate it.

Theorem 31. *For any rational number $r \neq 0$ the number e^r is irrational.*

Lemma 32. *Let n be a positive integer and set*

$$f(x) = \frac{x^n(1-x)^n}{n!}.$$

Then

(a) $f(x)$ is a polynomial of the form

$$f(x) = \frac{1}{n!}\sum_{k=n}^{2n} c_k x^k$$

where the coefficients c_k are integers.

(b) For $0 < x < 1$

$$0 < f(x) < \frac{1}{n!}.$$

(c) The derivatives $f^{(k)}(0)$ and $f^{(k)}(1)$ are integers for all $k \geq 0$.

Problem 25. Prove this. *Hint:* For (a) this follows by expanding $(1-x)^n$ be the binomial theorem. For (b) use that $0 < x(1-x) \leq 1/4$ for $0 < x < 1$ and therefore $f(x) = \big(x(1-x)\big)^n/n! \leq (1/4)^n/n!$. For (c) note that the lowest power of x that appears in $f(x)$ is x^n which implies $f^{(k)}(0) = 0$ for $k < n$. For $k \geq n$ we have $f^{(k)}(0) = \frac{k!}{n!}c_k$ which is the product of the two integers c_k and $\frac{k!}{n!} = (n+1)(n+2)\cdots k$. Finally show $f(1-x) = f(x)$ and therefore $f^{(k)}(1) = (-1)^k f^{(k)}(0)$. □

Problem 26. Prove Theorem 31 along the following lines.

(a) Explain why it is enough to show e^ℓ is irrational for all integers ℓ. *Hint:* If $r = \ell/m$ and e^r is rational then $e^\ell = (e^r)^m$ would also be rational.

Towards a contradiction assume e^ℓ is rational, say

$$e^\ell = \frac{a}{b},$$

with a and b integers.

(b) Explain why there is an integer n such that

$$\frac{a\ell^{2n+1}}{n!} < 1.$$

(c) For this n let $f(x)$ be the polynomial of Lemma 32 and set

$$F(x) := \ell^{2n}f(x) - \ell^{2n-1}f'(x) + \ell^{2n-2}f''(x) - \ell^{2n-3}f^{(3)}(x) \pm \cdots + f^{(2n)}(x).$$

As $f(x)$ has degree $2n$ we have $f^{(2n+1)}(x) = 0$. Use this to show

$$F'(x) + \ell F(x) = \ell^{2n+1}f(x).$$

(d) Use this to show

$$\frac{d}{dx}\left(e^{\ell x}F(x)\right) = \ell e^{\ell x}F(x) + e^{\ell x}F'(x) = \ell^{2n+1}e^{\ell x}f(x).$$

(e) Set

$$N := b \int_0^1 \ell^{2n+1} e^{\ell x} f(x)\, dx$$

and justify the following calculation

$$\begin{aligned} N &= b \int_0^1 \frac{dF}{dx} \left(e^{\ell x} F(x) \right) dx \\ &= b e^{\ell x} F(x) \Big|_{x=0}^{1} \\ &= b e^{\ell} F(1) - b F(0) \\ &= a F(1) - b F(0). \end{aligned}$$

(f) Show N is a positive integer. *Hint:* Lemma 32.
(g) Explain why the following holds:

$$0 < N = b \int_0^1 \ell^{2n+1} e^{\ell x} f(x)\, dx < b \ell^{2n+1} e^{\ell} \frac{1}{n!} = \frac{a \ell^{2n+1}}{n!} < 1.$$

Hint: For the first inequality note N is the integral of a positive function. For the second inequality if $0 < x < 1$ we have $e^{\ell x} \leq e^{\ell}$ and, by Lemma 32, $f(x) < 1/n!$. For the third inequality see part (b).
(h) Combine parts (f) and (g) to get a contradiction. □

This same idea can be used to show that π is irrational.

Theorem 33. *The number π is irrational.*

Problem 27. Here as an outline of a somewhat more general result, that π^2 is irrational. This argument is due to Ivan Niven from 1947. We start by assuming that π^2 is rational, say

$$\pi^2 = \frac{a}{b}$$

where a and b are positive integers. Let n be a positive ingteger to be chosen later, and $f(x)$ be the polynomial from Lemma 32. Set

$$F(x) = b^{2n} \left(\pi^{2n} f(x) - \pi^{2n-2} f^{(2)(x)} + \pi^{2n-4} f^{(4)}(x) - \pi^{2n-6} f^{(6)}(x) + \cdots \right)$$

While this is formally an infinite sum, not $f(x)$ has degree $2n$ and therefore $f^{(k)}(x) = 0$ for $k > 2n$. Thus this is really only a finite sum.

(a) Use Lemma 32 and $\pi^2 = a/b$ to show both $F(0)$ and $F(1)$ are integers.
(b) Show F satisfies

$$F''(x) + \pi^2 F(x) = b^n \pi^{2n+2} f(x).$$

(c) Justify the following calculation

$$\begin{aligned}\frac{d}{dx}\left(F'(x)\sin\pi x - \pi F(x)\cos\pi x\right) &= \left(F''(x) + \pi^2 F(x)\right)\sin\pi x \\ &= b^n\pi^{2n+2} f(x)\sin\pi x \\ &= \pi^2 a^n f(x)\sin\pi x\end{aligned}$$

(d) Set

$$N = \int_0^1 \pi a^n f(x)\sin\pi x\,dx$$

Then by (c)

$$N = \frac{1}{\pi}\int_0^1 \frac{d}{dx}\left(F'(x)\sin\pi x - \pi F(x)\cos\pi x\right)\,dx.$$

Use this to show

$$N = F(0) + F(1)$$

and therefore N is a positive integer. *Hint:* For showing N is positive note $\pi a^n f(x)\sin\pi x$ is positive for $0 < x < 1$ and N is an integral of this function.

(e) Use Lemma 32 to show

$$N < \int_0^1 \pi a^n \frac{1}{n!}\sin\pi x\,dx = \frac{2a^n}{n!}.$$

(f) We have yet to choose n. Show that it is possible to choose n such that

$$\frac{2a^n}{n!} < 1$$

which leads to the contradiction that N is an integer between 0 and 1. This finishes the proof. □