1.3: Suppose $p_1, \ldots, p_n$ are all the primes of the form $6x-1$. Consider $N = 6p_1 \cdots p_n - 1$. If $p_i | N$ for some $p_i$, then $p_i | 1$, so none of the $p_i$ can divide $N$. It’s also clearly not divisible by 2 or 3. So $N$ is only divisible by primes of the form $6x + 1$. But any product of numbers of the form $6x + 1$ is again of the form $6x + 1$, and $N$ is not of that form: a contradiction.

1.8: (b) Since $\gcd(a, b) = 1$, there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying by $c$, we have $acx + bcy = c$. Since $a|bc$, we have $a|bcy$, and it’s clear that $a|acx$, so $a|c$.

(a) Since $b|n$, we have $n = bk$ for some $m \in \mathbb{Z}$. So $a|bm$. We have $\gcd(a, b) = 1$, so by part (b), $a|m$. Say $m = ak$. Then $n = abk$, so $ab|n$.

1.9: (a) $c = kb$ for some $k$ and $b = ma$ for some $m$, so $c = (km)a$, so $a|c$.

(b) $b = ka$ and $d = mc$ for some $k$ and $m$, so $bd = (km)(ab)$, so $ab|bd$.

(c) If $b = ka$ for some $k$, then $mb = kma$, so $ma|mb$. Conversely, if $mb = kma$ for some $k$, then $b = ka$ since $m \neq 0$, so $a|b$.

(d) Suppose $a = kd$ for some $k \in \mathbb{Z}$. Then $|a| = |k| \cdot |d|$. Since $a \neq 0$, we must have $k \neq 0$, so $|k| \geq 1$. So $|a| \geq |d|$.

1.12: Note that $x|y$ if and only if for every prime $p$, the largest power of $p$ appearing in the prime factorization of $x$ is less than or equal to the the largest power of $p$ appearing in $y$.

(a) For a given prime $p$, suppose $p^f$ is the largest power of $p$ dividing $a$ and $p^d$ is the largest power of $p$ dividing $b$. Then $p^{nc}$ is the largest power of $p$ dividing $a^n$ and $p^{nd}$ is the largest power of $p$ dividing $b^n$. Since $a^n|b^n$, we have that $nc \leq nd$. Since $n$ is positive, we have that $c \leq d$.

(b) Suppose $p^f$ is the largest power of $p$ dividing $a$. Since $p^k|a^k$, we have that $0 < 1 \leq kc$. Since $k$ is positive, we have $0 < c$. Since $c$ is an integer, $1 \leq c$, so $p|a$.

1.13: (a) Check that $(4m)^2 = 4(4m^2)$, $(4m + 1)^2 = 4(4m^2 + 2m) + 1$, $(4m + 2)^2 = 4(4m^2 + 4m + 1)$, and $(4m + 3)^2 = 4(4m^2 + 6m + 2) + 1$. Since every integer is of the form $4m + i$ for $i = 0, 1, 2,$ or $3$, this shows that the remainder of a square upon division by 4 is always 0 or 1. It cannot be 3.

(b) $111 \cdots 111 = 111 \cdots 108 + 3 = 4(111 \cdots 1 \times 25 + 2) + 3$, so by (a) it cannot be a square.

1.14: If $n$ is prime, then it is clearly not divisible by any prime $p$ with $1 < p \leq \sqrt{n}$ since it is not divisible by any number strictly between 1 and $n$ ($\sqrt{n} < n$ since 2 is the smallest prime). On the other hand, if $n$ is not prime, then $n = ab$ for some integers $a, b > 1$. If $a, b > \sqrt{n}$, then $n > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction. So one of $a$ or $b$ is less than or equal to $\sqrt{n}$, say $1 < a \leq \sqrt{n}$. Let $p$ be any prime divisor of $a$. Then $1 < p$ since $p$ is prime, and by 1.9(d), $p \leq a$, so $1 < p \leq \sqrt{n}$.

1. The gcd is 61:

- $4819 - 1 \times 4087 = 732$
- $4087 - 5 \times 732 = 427$
- $732 - 1 \times 427 = 305$
- $427 - 1 \times 305 = 122$
- $305 - 2 \times 122 = 61$
- $122 - 2 \times 61 = 0$
This gives that
\[
\frac{4819}{4087} = 1 + \frac{1}{5 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}}}.
\]

2. It’s false. Take \(a = d = 1\) and \(b = c = 2\), then \(\gcd(ac, bd) = \gcd(2, 2) = 2\), but \(\gcd(a, b) = \gcd(c, d) = \gcd(1, 2) = 1\).

3. (a) Let \(n\) be an element of \(\mathbb{E}\) with minimal absolute value which cannot be factored into \(\mathbb{E}\)-primes (such an element exists if there is any element of \(\mathbb{E}\) with no \(\mathbb{E}\)-prime factorization). If \(n\) cannot be factored as \(ab\) where \(a, b \in \mathbb{E}\), then it is \(\mathbb{E}\)-prime so \(n = n\) is an \(\mathbb{E}\)-prime factorization: a contradiction. So we have \(n = ab\) for some \(a, b \in \mathbb{E}\). Since \(n \neq 0\), \(a, b \neq 0\), so \(|a|, |b| \geq 2\), so \(|a|, |b| < |n|\). Since \(n\) had minimal absolute value among elements of \(\mathbb{E}\) with no \(\mathbb{E}\)-prime factorization, \(a\) and \(b\) have \(\mathbb{E}\)-prime factorizations. The product of these is an \(\mathbb{E}\)-prime factorization of \(n\): a contradiction. So there is no \(n \in \mathbb{E}\) with no \(\mathbb{E}\)-prime factorization.

(b) No. \(2, 6, \) and \(18\) are all \(\mathbb{E}\)-prime (see next part), but \(2 \cdot 18 = 6 \cdot 6\).

(c) For any even number \(n\), let \(2^k\) be the largest power of 2 dividing \(n\) (in \(\mathbb{Z}\)); say \(n = 2^km\).
Since \(n\) is even, \(k \geq 1\). If \(k \geq 2\), then \(n = 2 \cdot 2^{k-1}m\) with \(2, 2^{k-1}m \in \mathbb{E}\), so \(n\) is not \(\mathbb{E}\)-prime. 
Conversely, if \(n = ab\) with \(a\) and \(b\) even, then \(4|n\), so \(k \geq 2\). Thus, the \(\mathbb{E}\)-primes are exactly the numbers which are divisible by 2 but not by 4 (in \(\mathbb{Z}\)). These are the numbers whose remainder upon division by 4 is 2. Every second even number is of this form, so 250,000,000 of the 500,000,000 even numbers up to a billion are \(\mathbb{E}\)-prime.

4. (a) True. If \(x \in \mathbb{Z}[i]\), let \(\bar{x}\) be the complex conjugate. Note that \(\bar{x}y = xy\bar{y}\) and that \(N(x) = x\bar{x}\). Now we have that \(N(xy) = xy\bar{y} = x\bar{x}\bar{y} = x\bar{y}y = N(x)N(y)\).

(b) True. Say \(N(x) = x\bar{x} = 1\), then \(\bar{x}\) is a multiplicative inverse of \(x\). Conversely, if \(y\) is a multiplicative inverse of \(x\), then \(1 = N(1) = N(xy) = N(x)N(y)\). Since \(N(x)\) and \(N(y)\) are positive integers, \(N(x) = N(y) = 1\).

Suppose \(x = a + ib\) is a unit, then \(1 = N(x) = a^2 + b^2\), so the only units are \(1, -1, i, \) and \(-i\).

(c) \(\mathbb{Z}[i]\) is a unit square grid in \(\mathbb{C}\). Note that any point in a unit square is within \(1/\sqrt{2}\) distance of a corner. Let \(q \in \mathbb{Z}[i]\) be a point which is within \(\sqrt{2}\) of the complex number \(y/x\). Then \(|y/x - q| \leq 1/\sqrt{2}\), so \(|y \pm qx| \leq |x|/\sqrt{2} < |x|\). It follows that \(N(y \mp qx) < N(x)\). Take \(r = y - qx\).

(d) They’re not unique. For example, if \(y = 3\) and \(x = 2\), we can take \(q = 1, r = 1\), or \(q = 2, r = -1\).

(e) Let \(d \in \mathbb{Z}[i]\) be an element of minimal positive norm in the set \(S = \{\alpha x + \beta y | \alpha, \beta \in \mathbb{Z}[i]\}\).
Say \(d = ax + by\). If \(z|x\) and \(z|y\), then clearly \(z|d\). For the converse, it’s enough to show that \(d|x\) and \(d|y\). Choose \(q, r \in \mathbb{Z}[i]\) such that \(x = qd + r\) with \(N(r) > N(d)\) (we can do this by part (c)). Then \(r = x - qd = (1 - aq)x + (\mp b)y \in S\). Since \(d\) had minimal positive norm among elements of \(S\), we must have that \(N(r) = 0\), so \(r = 0\), so \(x = qd\), so \(d|x\). Similarly \(d|y\).
(f) If \( x = ab \) for non-units \( a, b \in \mathbb{Z}[i] \), then \( N(x) = N(a)N(b) \), with \( N(a), N(b) > 1 \). So if any proper factorization of \( N(x) \) involves a number which cannot be written as the sum of two squares, then \( x \) must be prime. The numbers 3, 7, and 11 cannot be written as a sum of two squares, and these appear in all proper factorizations of \( N(3) = 9, N(7) = 49, N(11) = 121 \), and \( N(1 + 3i) = 10 \), so those numbers are prime. \( N(1 + 2i) = 5 \) and \( N(1 + i) = 2 \) have no proper factorizations, so those numbers are prime. The rest can be factored into non-units: 2 = (1 + i)(1 − i), 5 = (1 + 2i)(1 − 2i), 6 = 2 · 3, and 1 + 3i = (−1 + 2i)(1 − i).

(g) Suppose \( p | xy \), but \( p \nmid x \). Choose \( d \) as in part (e). Since \( p \) is prime and \( d | p \), \( d \) is either a unit or a unit multiple of \( p \), but since \( d | x \) and \( p \nmid x \), \( d \) must be a unit. Say \( ax + bp = d \), then \( ad^{-1}x + bd^{-1}p = 1 \). Multiplying through by \( y \), we have \( ad^{-1}xy + bd^{-1}yp = y \). Since \( p | xy \) we have \( p | ad^{-1}xy \), and clearly \( p | bd^{-1}yp \), so \( p | y \).

(h) Suppose \( n \in \mathbb{Z}[i] \) is an element of smallest positive norm which cannot be factored into primes times units, if there is one. If \( N(n) = 1 \), then \( n \) is a unit, so \( n = n \) is a factorization. If \( n \) is prime, then \( n = n \) is a factorization. So we may assume \( n \) is not a unit or a prime. Let \( n = ab \) be a factorization into non-units, then \( 0 < N(a), N(b) < N(n) \), so \( a \) and \( b \) can be factored into primes. The product of these factorizations is a prime factorization of \( n \): a contradiction. So every non-zero \( n \in \mathbb{Z}[i] \) can be factored into primes. Now let \( m \in \mathbb{Z}[i] \) be an element of smallest positive norm which has two prime factorizations which are not the same up to reordering and multiplication by units. Say \( p_1p_2 \cdots p_k = m = q_1q_2 \cdots q_r \). By repeated application of part (g), \( p_1 \) must divide some \( q_i \). Since \( q_i \) is prime, \( p_1 = uq_i \) for some unit \( u \). But then up_2 \cdots p_k = m/p_1 = q_1 \cdots q_{i-1}q_{i+1} \cdots q_k \) are two factorizations of \( m/p_1 \) which are not the same up to reordering and multiplication by units. Since \( 0 < N(m/p_1) < N(m) \), this is a contradiction, so there is no \( m \) with two really different prime factorizations.