Sam Grayson's Notebook (with LaTeX)

March 12, 2015

2.1 Theorem: $n \in \mathbb{N} \wedge n \neq 1 \rightarrow \exists p(p \in \mathbb{P} \wedge p \mid n)$

But first, Prime or composite lemma: Any natural number p greater than one is either prime or composite. In other words if p is not composite, it is prime. If p is not prime, it is composite.

Every now and then, I feel I need to prove one thing formally so I don't get to relaxed with my form.

p is not composite	Premise
$\neg\exists a, b \in \mathbb{N}(p = ab \wedge 1 < a, b < p)$	Definition of composite (negated)
$\neg\exists a, b \in \mathbb{N}(p = ab \wedge 1 < a < p)$	Simplification
$\forall a, b \in \mathbb{N}\neg(p = ab \wedge 1 < a < p)$	Quantifier exchange
$\neg(p = ab \wedge 1 < a < p)$	Universal instantiation
$\neg(p = ab) \wedge \neg(1 < a < p)$	DeMorgan's law
$p = ab \rightarrow \neg(1 < a < p)$	Conditional disjunction
$p = ab \rightarrow \neg(1 < a \wedge a < p)$	Property of inequality
$p = ab \rightarrow \neg(1 < a) \vee \neg(a < p)$	DeMorgan's law
$p = ab \rightarrow 1 \geq a \vee a \geq p$	Property of inequality
$p = ab \rightarrow (1 = a \wedge a \geq p)$	Property of Natural numbers
$p = ab \rightarrow (1 = a \wedge a = p)$	$a \mid p \rightarrow a \leq p$
$a \mid p \rightarrow (1 = a \wedge a = p)$	Definition of division
$\forall a(a \mid p \rightarrow (1 = a \vee a = p))$	Universal generalization
p is prime	Definition of primes ■

$p \in \mathbb{P}$	Premise
$\neg(\forall d(d \mid n \rightarrow (d = 1 \vee d = n)))$	Definition of prime
$\exists d\neg(d \mid n \rightarrow (d = 1 \vee d = n))$	Quantifier exchange
$\exists d\neg(\neg(d \mid n) \vee (d = 1 \vee d = n))$	Conditional disjunction
$\exists d\neg\neg(d \mid n) \wedge \neg(d = 1 \vee d = n)$	DeMorgan's law
$\exists d(d \mid n \wedge \neg(d = 1 \vee d = n))$	Double Negation
$\exists d(d \mid n \wedge d \neq 1 \wedge d \neq n)$	DeMorgan's law
$\exists d(d \mid n \wedge 1 < d < n)$	Inequality over naturals
$\exists d\exists c(cd = n) \wedge 1 < d < n$	Definition of divides
$\exists d\exists c(cd = n \wedge 1 < c < n) \wedge 1 < d < n$	Inequality over naturals
p is composite ■	

Because of this, let $a \notin \mathbb{P}$ stand for 'a is composite' (only when $a \neq 1$).

Transitivity of divisibility Lemma: $a \mid b \wedge b \mid c \rightarrow a \mid c$

$an = b$	Definition of divides
$bm = c$	Definition of divides
$anm = c$	Substitution
$a \mid c$	Definition of divides ■

Theorem: $n \in \mathbb{N} \land n \neq 1 \to \exists p(p \in \mathbb{P} \land p \mid n)$

Assume: $p \in \mathbb{P}$	
$p = 1p$	Identity of Multiplication
Conclude: $p \mid p$	Definition of divides $\square$
Otherwise: $p \notin \mathbb{P}$	
Follow this algorithm:	
Initial step:	
$p = a_1 b_1 \land 1 < a_1, b_1 < p$ for some a_1, b_1	Definition of composite ($\notin \mathbb{P}$)
$a_1 \mid p$	Definition of divides
If $a_1 \in \mathbb{P}$: halt	
Otherwise: $a_1 \notin \mathbb{P}$	
$a_1 = a_2 b_2 \land 1 < a_2 < a_1 < p$	Definition of composite
Repeat with $a_1 \leftarrow a_2$	
ith step	
$a_i = a_{i+1} b_{i+2} \land 1 < a_i < a_{i-1} < \underbrace{\ldots}_{i \text{ times}} < p$	Definition of composite
$a_{i+1} \mid a_i$	Definition of divides
If $a_i \in \mathbb{P}$ halt	
Otherwise $a_i \notin \mathbb{P}$ and repeat	
Result:	
$a_{n-1} = a_n b_n \land 1 < a_n < \underbrace{\ldots}_{p \text{ times}} < p$	
There can not be p unique numbers between 1 and p	
Therefore this process must terminate (call that place a_j)	Algorithm halts
$a_j \in \mathbb{P} \land a_j \mid a_{j-1} \land a_{j-1} \mid a_{j-2} \land \ldots \land a_1 \mid p$	Condition for termination
$a_j \in \mathbb{P} \land a_j \mid p$	Transitivity of divisibility lemma ■

2.2 $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$

2.3 Theorem: $n \in \mathbb{P} \leftrightarrow \neg\exists p(p \in \mathbb{P} \land 1 < p \leq \sqrt{n} \land p \mid n)$

I will simply prove the biconditional with both sides negated.

Theorem equivalent: $n \notin \mathbb{P} \leftrightarrow \exists p(p \in \mathbb{P} \land 1 < p \leq \sqrt{n} \land p \mid n)$

$\to$

$n \notin \mathbb{P}$	Premise
$ab = n$ for some $1 < a, b < n$	Definition of $\notin \mathbb{P}$
Assume the following for contradiction	
$a > \sqrt{n}$	Assume
$b > \sqrt{n}$	Assume
$n > 1$	Premise
$\sqrt{n} > 1$	Property of square root
$a > \sqrt{n} > 1$	
$b > \sqrt{n} > 1$	Property of inequality
$ab > n$	Property of inequality (since they are all greater than 1)
$ab = n$	Definition of a and b

$\neg(a > \sqrt{n}) \vee \neg(b > \sqrt{n})$	Contradiction
$a \leq \sqrt{n} \vee b \leq \sqrt{n}$	Property of inequality
Either way:	
$\exists p(1 < p \leq \sqrt{n} \in \mathbb{N})$	Existential instantiation (on a or on b) $\blacksquare$

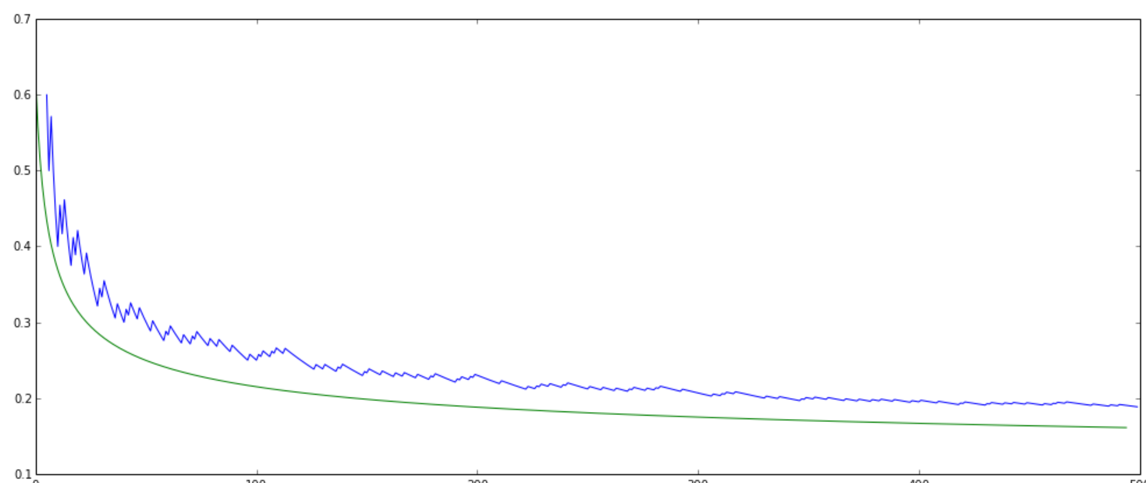
$\leftarrow$

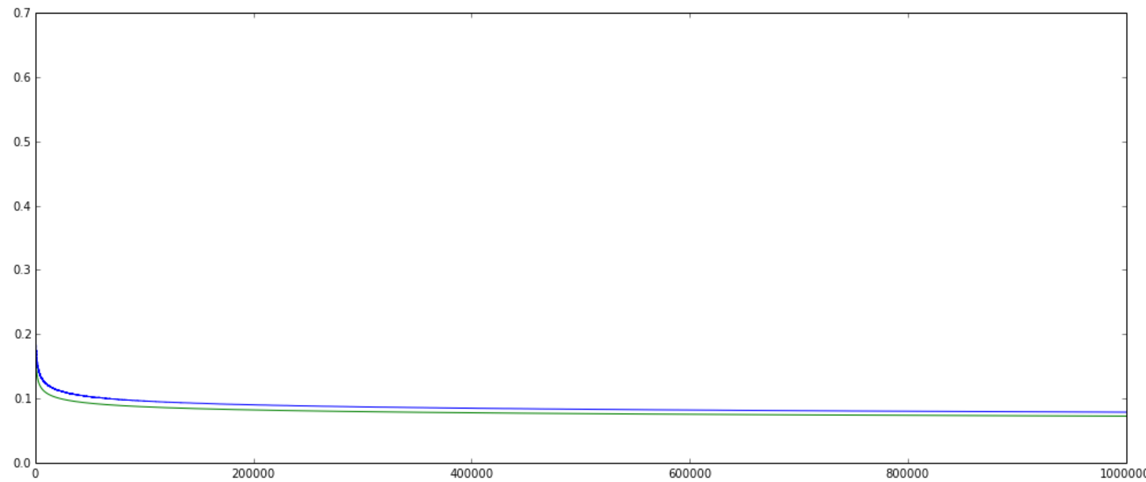
$p \in \mathbb{P} \wedge 1 < p \leq \sqrt{n} \wedge p \mid n$	Universal instantiation
$\sqrt{n} < n$	Property of positive numbers
$1 < p < n$	Property of inequalities
$\exists c(1 < c < n \wedge pc = n)$	Definition of divides
$1 < p, c < n \wedge pc = n$	Restatement
$n \notin \mathbb{P}$	Definition of composite $\blacksquare$

2.4 $101 < 121$
$\sqrt{101} < \sqrt{121}$ since they are all positive
$\sqrt{101} < 11$
$\{p \mid p \in \mathbb{P} \wedge p < 11\} = \{2, 3, 5, 7\}$
$2 \nmid 101 \wedge 3 \nmid 101 \wedge 5 \nmid 101 \wedge 7 \nmid 101$
$\therefore 101 \in \mathbb{P}$

2.5 $\{2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, 31, \cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, 37, \cancel{38}, \cancel{39}, \cancel{40}, 41, \cancel{42}, 43, \cancel{44}, \cancel{45}, \cancel{46}, 47, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, \cancel{55}, \cancel{56}, \cancel{57}, \cancel{58}, 59, \cancel{60}, 61, \cancel{62}, \cancel{63}, \cancel{64}, \cancel{65}, \cancel{66}, 67, \cancel{68}, \cancel{69}, \cancel{70}, 71, \cancel{72}, 73, \cancel{74}, \cancel{75}, \cancel{76}, \cancel{77}, \cancel{78}, 79, \cancel{80}, \cancel{81}, \cancel{82}, 83, \cancel{84}, \cancel{85}, \cancel{86}, \cancel{87}, \cancel{88}, 89, \cancel{90}, \cancel{91}, \cancel{92}, \cancel{93}, \cancel{94}, \cancel{95}, \cancel{96}, 97, \cancel{98}, \cancel{99}, \cancel{100}\}$

2.6 The blue line is $\frac{\Pi(x)}{x}$.
The green line is $\frac{1}{\ln(x)}$





2.7 Every natural number n excluding one can be written as the product of primes $\{p_1, p_2, \dots, p_m\}$ raised to natural-number powers $\{t_1, t_2, \dots, t_m\}$. (In other words $n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$.)

$n \in \mathbb{N} \land n \neq 1$	Premise
$\exists p_1(p_1 \mid n)$	Theorem 2.1
$\frac{n}{p_1} = 1 \lor \frac{n}{p_1} \neq 1$	Excluded Middle
	$\frac{n}{p_1}$ is legal since $p_1 \vert n$
Assume: $\frac{n}{p_1} = 1$	
Conclude: $n = p_1$	Algebra
Otherwise: $\frac{n}{p_1} \neq 1$	
Conclude: $\exists p_2(p_2 \mid \frac{n}{p_1})$	Theorem 2.1
Follow this algorithm:	
Initial step:	
If $\frac{n}{p_1 p_2} = 1$:	
Conclude: $p_1 p_2 = n$	
Otherwise: $\exists p_3(p_3 \mid \frac{n}{p_1 p_2})$	Theorem 2.1 Repeat with $\frac{n}{p_1 p_2} \leftarrow \frac{n}{p_1 p_2 p_3}$
***i*th step:**	
If $\frac{n}{p_1 p_2 \dots p_i} = 1$:	
Conclude: $p_1 p_2 \dots p_i = n$	
Otherwise: $\frac{n}{p_1 p_2 \dots p_i} \neq 1$	
$\exists p_{i+1}(p_{i+1} \mid \frac{n}{p_1 p_2})$	Theorem 2.1
Result:	
Each iteration, n decreases.	
Therefore the algorithm halts.	
$p_1 p_2 \dots p_m = n$	Halting condition ■

2.8 Coprime primes lemma: any prime number (p) is coprime to any other prime number (q).

$p \in \mathbb{P} \land q \in \mathbb{P} \land p \neq q$	Premise
$\gcd(p, q) \mid p \land \gcd(p, q) \mid q$	Definition of GCD
$(a = 1 \lor a = q) \land (a = 1 \lor a = p)$	Definition of prime
$a = 1 \lor a = p = q$	Simplification
$p \neq q$	Premise

$a = 1$ Disjunctive syllogism ■

$p \neq 1$	Premise
$p \mid (\prod_{i=1}^{n} q_i)$	Definition of divides
$\forall i\{q_i \neq p\}$	Assume for contradiction
$\forall i\{(q_i, p) = 1\}$	Coprime primes lemma (applied over all p_i)
$p \mid q_1 \prod_{i=2}^{n} q_i$	Algebra
$(p, q_1) = 1$	Coprime primes lemma
$p \mid \prod_{i=2}^{n} q_i$	Theorem 1.41 (Base case)
$p \mid \prod_{i=j}^{n} q_i$	Assume (Inductive hypothesis)
$p \mid q_{j+1} \prod_{i=j+1}^{n} q_j$	Algebra
$(p, q_j) = 1$	Coprime primes lemma
$p \mid \prod_{i=j+1}^{n}$	Theorem 1.41 (Inductive Step)
$p \mid \prod_{i=n}^{n}$	Inductive axiom
$p \mid 1 \wedge p \neg \mid 1$	Product rule
$\neg\forall i\{q_i \neq p\}$ Contradiction	
$\exists i\{q_i = p\}$	Simplification ■

2.9 Every natural number excluding one has a **unique** prime factorization.

$\forall_{n \in \mathbb{N}\setminus\{1\}}(\exists_{\{p_1,p_2,\ldots,p_n\}\subset\mathbb{P}}\ \exists_{\{r_1,r_2,\ldots,r_n\}\subset\mathbb{N}}\exists_{\{q_1,q_2,\ldots,q_m\}\subset\mathbb{P}}\ \exists_{\{t_1,t_2,\ldots,t_m\}\subset\mathbb{N}}(\prod^{i} p_i^{r_i} = \prod^{j} q_j^{t_j}) \to m = n \wedge \{p_1, p_2, \ldots, p_n\} = \{q_1, q_2, \ldots, q_m\} \wedge (p_i = q_j \to r_i = t_j))$

2.10
$$\begin{aligned} 12! &= 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \\ &= 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) \cdot 11 \cdot (2^2 \cdot 3) \\ &= 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \end{aligned}$$

2.11 $25! = 1 \cdot 2 \cdot 3 \ldots 25$
The largest power of 5 that divides 25 is 5^{5+1}
The largest power of 2 that divides 25 is $2^{12+5+3+1}$
$5^{5+1} \cdot 2^{12+5+3+1} \mid 25$
$5^6 \cdot 2^{21} \mid 25$
$10^6 \cdot 2^{21-6} \mid 25$
The largest power of 10 that divides 25 is 10^6
There are 6 zeros at the end of 25!

2.12 $a \mid b \leftrightarrow \mathrm{pf}(a) \subseteq \mathrm{pf}(b)$
Let $\mathrm{pf}(a) = A, \mathrm{pf}(b) = B$
$\to$
$a \mid b$ Premise

$ma = b$ for some $m \in \mathbb{Z}$	Definition of divides
Let $pf(m) = M$ $\text{pf}(ma) = B$	pf uniqueness
$M + A = B$	pf of product theorem
$A \subseteq B$	addend-subset theorem $\blacksquare$

$\leftarrow$

$A + (B - A) = B$	Definition of list-subtraction
$\text{pf}(a \cdot \prod(\text{pf}(b) - \text{pf}(a)) = b$	pf of product
$a \cdot \prod \text{pf}(b) - \text{pf}(a) = b$	Uniquness of pf
$a \mid b$ $\blacksquare$	

2.13 $\text{pf}(a^2) \subseteq \text{pf}(b^2) \rightarrow \text{pf}(a) \subseteq \text{pf}(b)$

$a = p_1^{r_1} p_2^{r_2} \ldots$	
$b = q_1^{t_1} q_2^{t_2} \ldots$	Fundamental Theorem of Arithmetic
$a^2 = p_1^{2r_1} p_2^{2r_2} \ldots$	
$b^2 = q_1^{2t_1} q_2^{2t_2} \ldots$	Algebra
$2r_1 \leq 2t_2$	Definition of subset
$r_1 \leq t_2$	Property of inequality
$\text{pf}(a) \subset \text{pf}(b)$	Definition of subset $\blacksquare$

2.14 $\gcd(3^14 \cdot 7^22 \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17) = 11^4 \cdot 17$

2.15 $\text{lcm}(3^14 \cdot 7^22 \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17) = 3^14 \cdot 5^2 \cdot 7^22 \cdot 11 \cdot 13^8 \cdot 17^2 \cdot 11^4 \cdot 17$

2.16 $\gcd(a, b) = \text{pf}(a) \cap \text{pf}(b)$

$\text{lcm}(a, b) = \text{pf}(a) \cup \text{pf}(b)$

2.17 It depends on how easy it is to factor. I easily recognize the prime factorization if and only if the prime factorization method is clearly better.

In general, factoring a number assuming the density of primes is proportional $\frac{1}{\ln(x)}$ as proposed in 2.6, the number of primes less than n should be $\int\limits_{x=1}^{x=n} \frac{1}{\ln(x)}\, dx = n\ln(n) - n - 1$. Lets assume I need to do long division to test for divisibility. Long division has complexity of $\mathcal{O}(log(x))$. Now for every prime, I need to do this check. The worst case scenario is that the number under test is itself prime, therefore the problem does not reduce as I continue (what normally happens when factoring). The worst-case run-time is $\mathcal{O}(log^2(n))$ where n is the number under test.

On the other hand, the Euclidean Algorithm replaces the larger number with the difference of the two. For the worst-case scenario, we will assume the difference is such that half the next term is close to half of the smaller term. Thus we divide by two every time. The worst-case run-time is $\mathcal{O}(log(n))$.

Because of this, I think the Euclidean Algorithm is more efficient as the n approaches ∞.

2.18 If $n = 1$, the theorem is true,
since there is only one number to pick from (**Base Case**)
The theorem holds for picking n numbers less than or equal to $\{1, \ldots 2n\}$ (**Inductive Hypothesis**)
Additionally assume it holds for picking all $k < n$ that picking n numbers less than or equal to $\{1, \ldots, 2$
We pick from $1 to 2n + 2$
We pick from $\{1, \ldots, 2n, 2n+1, 2n+2\}$
There are three options:
First, we can pick $n + 1$ numbers from $\{1, \ldots, 2n$
Second, we can pick n numbers from $\{1, \ldots, 2n\}$ and 1 number from $\{2n + 1, 2n + 2\}$
Third, we can pick $n - 1$ numbers from $\{1, \ldots, 2n\}$ and both $\{2n + 1, 2n + 2\}$
In the first case, the theorem holds, by the Inductive Hypothesis
In the second case, the theorem holds by the Inductive Hypothesis
In the third case, either $n + 1$ is among the chosen (case 3a) or $n + 1$ is not (case 3b)
In the 3a case, $(n + 1) \mid (2n + 1)$

2.19 $\neg\exists m, n(7m^2 = n^2)$

$7m^2 = n^2$ for some $m, n \in \mathbb{N}$	Assume for contradiction
$\mathrm{pf}(7m^2) = \mathrm{pf}(n^2)$	Uniqueness of pf
$\mathrm{pf}(7) + \mathrm{pf}(m^2) = \mathrm{pf}(n^2)$	pf of product
$\mathrm{pf}(7) = \{7\}$	
$\lvert\mathrm{pf}(7) + \mathrm{pf}(m^2)\rvert = \lvert\mathrm{pf}(n^2)\rvert$	Cardinality of equal lists
$\lvert\mathrm{pf}(7)\rvert + \lvert\mathrm{pf}(m^2)\rvert = \lvert\mathrm{pf}(n^2)\rvert$	Cardinality of sum
$\lvert\mathrm{pf}(7)\rvert + 2\lvert\mathrm{pf}(m)\rvert = 2\lvert\mathrm{pf}(n)\rvert$	Cardinality of power
$1 + 2\lvert\mathrm{pf}(m)\rvert = 2\lvert\mathrm{pf}(n)\rvert$	
$1 = 2(\lvert\mathrm{pf}(n)\rvert - \lvert\mathrm{pf}(m)\rvert)$	Algebra
$2 \lvert 1$	Definition of divides
	Contradiction of known fact
$\neg\exists m, n7m^2 = n^2$	Contradiction ■

2.20 $\neg\exists m, n(24m^3 = n^3)$

The heart of the proof of 2.19 is that if you prime factorize is that on the left-hand side you have a number whose prime factorization contains 7 and m^2 (an odd number of factors). On the right hand side the prime factorization is n^2 (an even number of factors). Since there is one unique way to prime-factorize numbers, it follows that these two different prime-factorizations do not represent the same number.

Similarly, if we let $24m^3 = n^3$, then $3 \cdot 2^3 m^3 = n^3$. The two cubed is fine. It can be absorbed into the n. But the three is 'left over'. There is only one way to factorize numbers and the left-hand side has an extra 3. If the right hand side contained a three, it would be three cubed, three to the sixth power, or three to the ninth power, etc. The left hand side would have to have three, three to the fourth, or three to the seventh, etc. It follows from the FTA that since the prime factorizations are different, the equality isn't true.

2.21 $\sqrt{7} \notin \mathbb{Q}$

$\sqrt{7} \in \mathbb{Q}$	Assume for contradiction
$\sqrt{7} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$	Definition of rational
$7n^2 = m^2$	Algebra

This contradicts theorem 2.19	
$\sqrt{7} \notin \mathbb{Q}$	Contradiction ∎

2.22 $\sqrt{12} \notin \mathbb{Q}$

$\sqrt{12} \in \mathbb{Q}$	Assume for contradiction
$\sqrt{12} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$	Definition of rational
$12n^2 = m^2$	Algebra
Let $n = n_0 n_1 n_2 \ldots$	
and $m = m_0 m_1 m_2 \ldots$	FTA
$32^2 n_0^2 n_1^2 n_2^2 \ldots = m_0^2 m_1^2 m_2^2 \ldots$	Substitution
$3n_0^2 n_1^2 n_2^2 \ldots = m_1^2 m_2^2 \ldots$	Theorem 2.8
$3n_1^2 n_2^2 \ldots = m_2^2 \ldots$	Theorem 2.8
$3n_1^2 n_2^2 \ldots = m_2^2 \ldots$	Theorem 2.8
Continuing this process	
$3 = 1$	Theorem 2.8
This contradicts known fact	
$\sqrt{12} \notin \mathbb{Q}$	Contradiction ∎

2.23 $\sqrt[3]{7} \notin \mathbb{Q}$

$\sqrt[3]{7} \in \mathbb{Q}$	Assume for contradiction
$\sqrt[3]{7} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$	Definition of rational
$7n^3 = m^3$	Algebra
$7n_0^3 n_1^3 n_2 n^3 \ldots = m_0^3 m_1^3 m_2^3 \ldots$	Theorem 2.8
$7n_0^3 n_1^3 n_2 n^3 \ldots = m_0^3 m_1^3 m_2^3 \ldots$	Theorem 2.8
$7n_1^3 n_2 n^3 \ldots = m_1^3 m_2^3 \ldots$	Theorem 2.8
$7n_2 n^3 \ldots = m_2^3 \ldots$	Theorem 2.8
Repeating this process	
$7 = 1$	Theorem 2.8
Contradiction	
$\sqrt[3]{7} \notin \mathbb{Q}$	Contradiction ∎

2.24 Let $n, x \in \mathbb{N}$. If $\sqrt[n]{x} \notin \mathbb{N} \to \sqrt[n]{x} \notin \mathbb{Q}$

$\sqrt[n]{x} \notin \mathbb{N}$	Premise
Assume $\sqrt[n]{x} \in \mathbb{Q}$	For contradiction
$\sqrt[n]{x} = \frac{j}{k}$ for some $j, k \in \mathbb{Z}$	Definition of rational
$xk^n = j^n$	Algebra
$xk_0^n k_1^n k_2^n \ldots = j_0^n j_1^n j_2^n \ldots$	FTA
$xk_1^n k_2^n \ldots = j_1^n j_2^n \ldots$	Theorem 2.8
$xk_2^n \ldots = j_2^n \ldots$	Theorem 2.8
Repeating this process	
Stop when all k are eliminated	
Lets call it the ith step	
$x = j_i^n j_{i+1}^n \ldots$	Theorem 2.8
$\sqrt[n]{x} = j_i j_{i+1}$	Algebra

$\sqrt[n]{x} \in \mathbb{N}$ Closure of $\mathbb{N}$ over multiplication
$\sqrt[m]{x} \notin \mathbb{Q}$ Contradiction $\blacksquare$

2.27 Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. $p \mid ab \to p \mid a \vee p \mid b$.

Let $\text{pf}(a) = A, \text{pf}(b) = B, \text{pf}(p) = P$

$P \subseteq \text{pf}(ab)$	Division-subset theorem
$P \subseteq \text{pf}(a) + \text{pf}(b)$	pf of product theorem
$p \in A + B$	Prime divisor theorem
Assume $p \mid a$	
$p \mid a \vee p \mid b$	Addition $\square$
Conclude: theorem holds	
Assume: $p \nmid a$	
$p \notin A$	Prime divisor theorem
$p \in B$	Element of disjunction
$p \mid b$	Prime divisor theorem
$p \mid a \vee p \mid b$	Addition $\square$
Conclude: theorem holds	
$p \mid a \vee p \mid b$	Either way (constructive dilemma) $\blacksquare$

2.28 $\gcd(b, c) = 1 \to \gcd(a, bc) = \gcd(a, b) \cdot \gcd(a, c)$

Let $\text{pf}(a) = A, \text{pf}(b) = B, \text{pf}(c) = C$

$B \cap C = \{\}$	Coprime-disjoint theorem
$\text{pf}(\gcd(a, b) \cdot \gcd(a, c))$	
$= \text{pf}(\gcd(a, b)) + \text{pf}(\gcd(a, c))$	Product of pf theorem
$= A \cap B + A \cap C$	GCD-intersection theorem
$\text{pf}(\gcd(a, bc))$	
$= A \cap \text{pf}(bc)$	GCD-intersection theorem
$= A \cap (B + C)$	Product of pf theorem
$= A \cap (B \cap C + B \cup C)$	Product of pf theorem
$= A \cap (\{\} + B \cup C)$	Substitution
$= A \cap (B \cup C)$	Identity property
$= A \cap B + A \cup C$	IDK
$\text{pf}(\gcd(a, b) \cdot \gcd(a, c)) = \text{pf}(\gcd(a, bc))$	Substitution
$\gcd(a, b) \cdot \gcd(a, c) = \gcd(a, bc)$	Uniqueness of pf $\blacksquare$

2.29 $\gcd(a, b) = 1 \wedge \gcd(a, c) = 1 \to \gcd(a, bc) = 1$

Let $\text{pf}(a) = A, \text{pf}(b) = B, \text{pf}(c) = C$

$A \cap B = \{\}$	
$A \cap C = \{\}$	Coprime-disjoint theorem
$\{\} + \{\} = A \cap B + A \cap C$	Substitution
$\{\} = A \cap B + A \cap C$	Identity
$\{\} = A \cap (B + C)$	IDK
$\{\} = A \cap \text{pf}(bc)$	pf of product
$\gcd(a, bc) = 1$	Coprime-disjoint theorem $\blacksquare$

2.30 $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$

Let $x \in \mathbb{P}$

$x\#\text{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) =$

$= x\#\text{pf}(\frac{a}{\gcd(a,b)}) \cap \text{pf}(\frac{b}{\gcd(a,b)})$	GCD-intersection theorem
$= x\#(\text{pf}(a) - \text{pf}(\gcd(a,b))) \cap (\text{pf}(b) - \text{pf}(\gcd(a,b)))$	pf of fraction theorem
$= x\#(\text{pf}(a) - \text{pf}(a) \cap \text{pf}(b)) \cap (\text{pf}(b) - \text{pf}(a) \cap \text{pf}(b))$	GCD-intersection theorem
$= \min(x\#\text{pf}(a) - x\#\text{pf}(a) \cap \text{pf}(b), x\#\text{pf}(b) - x\#\text{pf}(a) \cap \text{pf}(b))$	Definition of intersection
$= \min(x\#\text{pf}(a) - x\#\text{pf}(a) \cap \text{pf}(b), x\#\text{pf}(b) - x\#\text{pf}(a) \cap \text{pf}(b))$	Definition of list subtraction
$= \min(x\#\text{pf}(a) - \min(x\#\text{pf}(a), x\#\text{pf}(b)),$ $x\#\text{pf}(b) - \min(x\#\text{pf}(a), x\#\text{pf}(b)))$	Definition of intersection
Assume $\min x\#pf(a), x\#\text{pf}(b) = x\#\text{pf}(a)$	
$= \min(x\#\text{pf}(a) - x\#\text{pf}(a), x\#\text{pf}(b) - x\#\text{pf}(a))$	Assumption
$= \min(0, x\#\text{pf}(b) - x\#\text{pf}(a))$	Algebra
$= 0$	Definition of min
Conclude $x\#\text{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$	
Otherwise $\min x\#pf(a), x\#\text{pf}(b) = x\#\text{pf}(b)$	
$= \min(x\#\text{pf}(a) - x\#\text{pf}(b), x\#\text{pf}(b) - x\#\text{pf}(b))$	Assumption
$= \min(x\#\text{pf}(a) - x\#\text{pf}(b)), 0$	Algebra
$= 0$	Definition of min
Conclude $x\#\text{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$	
$x\#\text{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$	Either way
$\text{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = \{\}$	Notation for list
$\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$	Coprime-disjoint theorem ∎

2.31 $\gcd(a,b) = 1 \wedge u \mid a \wedge v \mid b \to \gcd(u,v) = 1$

Let $\text{pf}(u) = U, \text{pf}(v) = V, \text{pf}(a) = A, \text{pf}(b) = B$

$U \subseteq A$	
$V \subseteq B$	Division-subset theorem
$A \cap B = \{\}$	Coprime-disjoint theorem
$\min(x\#A, x\#B) = 0$	Notation for list
$\min(x\#A, x\#B) = x\#A \vee \min(x\#A, x\#B) = x\#B$	Definition of min
$x\#A = 0 \vee x\#B = 0$	Substitution
$x\#U \leq x\#A$	
$x\#V \leq x\#B$	Definition of subset
$x\#U \leq 0 \vee x\#V \leq 0$	Substiution
$x\#U = 0 \vee x\#V = 0$	Inequality over $\mathbb{W}$
$\min(x\#U, x\#V) = 0$	Definition of min
$U \cap V = \{\}$	Definition of intersection
$\gcd(u,v) = 1$	Coprime-disjoint theorem ∎

2.32 $\forall n \in \mathbb{N}(\gcd(n, n+1) = 1)$

Let $\gcd(n, n+1) = d$

$d \in \mathbb{N}$	Definition of gcd
$d \mid n$	
$d \mid (n+1)$	Definition of gcd

$ad = n$	
$bd = n$	Definition of divides
$n = n$	Identity
$n < n + 1$	Property of inequality
$ad < bd$	Substitution
$a < b$	Property of inequality
$b - a \geq 1$	Property of inequality over $\mathbb{W}$
$(b - a)d \geq d$	Property of inequality
$bd - ad \geq d$	Algebra
$n + 1 - n \geq d$	Substitution
$1 \geq d$	Algebra
$1 = d$	Property of inequality over $\mathbb{N}$ ∎

2.33 Let k be a natural number greater than 1. $\exists n \forall b (1 < b \leq k \rightarrow b \nmid n)$

GCD-divides Lemma: $\gcd(a, b) = a \leftrightarrow a \mid b$

$\rightarrow \gcd(a, b) = a$	Premise
$\gcd(a, b) \mid b$	Definition of GCD

$\leftarrow$

$a \mid b$	Premise
$1a = a$	Identity property
$a \mid a$	Definition of divides
$\gcd(a, b) \geq a$	Definition of GCD (a is a common factor)
$\gcd(a, b) \leq a$	Definition of GCD
$\gcd(a, b) = a$	Property of inequality ∎

Let $a = \prod\{p \mid p \in \mathbb{P} \wedge p \leq k\}$

$k > 1$	Premise
$a \geq 2$	Definition of a (with lower bound on k)
Let b be any integer where $1 < b \leq k$	
$\exists p \in \mathbb{P}(p \mid \gcd(b, a + 1))$	Assume for contradiction
$p \mid \gcd(b, a + 1)$	Premise for p
$\gcd(b, a + 1) \mid (a + 1)$	Definition of GCD
$p \mid (a + 1)$	Transitivity of divides
$p \mid a$	Theorem 1.3 (noting that a was the product of primes including p)
$p = 1$	Theorem 2.32
$1 \notin \mathbb{P}$	Contradicts premise for p
$\gcd(b, a + 1) = 1$	Contradiction
$b \neq 1$	Premise for b
$b \nmid (a + 1)$	GCD-divides lemma
$n = a + 1$ ∎	

2.34 There exists a prime larger than k for all $k > 1$.

There exists a number n that is coprime to every number below k.

Let b be any integer where $1 < b \leq k$

$\exists n \forall b(1 < b \leq k \to b \nmid n)$	Theorem 2.33
$\forall b(1 < b \leq k \to b \nmid n)$	Existantial instantiation
$1 < b \leq k \to b \nmid n$	Universal instantiation
$b \mid n \to b > k$	Contrapositive
$\forall b(b \mid n \to b > k)$	Universal generalization
$\exists p(p \mid n)$	FTA (2.7)
$p \mid n$	Universal instantiation
$p \mid n \to p > k$	Universal instantiation
$p > k$	Modus ponens ■

2.35 There are infinitely many primes.

I don't think this requires a proof seperate from theorem 2.34. I will however restate the proof of 2.34 and show that it is equivalent to the infinitude of primes.

If there were not an infinite number of primes, take the largest prime and use Theorem 2.33 to make a k that is not divisible by numbers less and including than the supposed largest prime. By the Fundamental Theorem of Arithmetic, that number is a product of primes. No primes are factors of that number. This implies a contradiction. Therefore there is no largest prime.

2.36 The most important setp is the claim $\gcd(a, a+1) = 1$. This is the initial seed that grows into the rest of the proof.

2.37 $r_1 \equiv 1 \pmod 4 \wedge r_2 \equiv 1 \pmod 4 \wedge \ldots \wedge r_m \equiv 1 \pmod 4 \to$

2.38

2.39

2.40 As of February 2015, the longest and largest known AP-k is an AP-26, found on February 19, 2015 by Bryan Little with an AMD R9 290 GPU using modified AP26 software. `http://primerecords.dk/aprecords.htm`

2.41