Notebook Swag

Sam Grayson

April 20, 2015

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

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.

Proof:

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

Proof:

$p \in \mathbb{P}$	Premise
$\neg(\forall d(d \mid n \to (d = 1 \lor d = n)))$	Definition of prime
$\exists d\neg(d \mid n \to (d = 1 \lor d = n))$	Quantifier exchange
$\exists d\neg(\neg(d \mid n) \lor (d = 1 \lor d = n))$	Conditional disjunction
$\exists d\neg\neg(d \mid n) \land \neg(d = 1 \lor d = n)$	DeMorgan's law
$\exists d(d \mid n \land \neg(d = 1 \lor d = n))$	Double Negation
$\exists d(d \mid n \land d \neq 1 \land d \neq n)$	DeMorgan's law
$\exists d(d \mid n \land 1 < d < n)$	Inequality over naturals
$\exists d\exists c(cd = n) \land 1 < d < n$	Definition of divides
$\exists d\exists c(cd = n \land 1 < c < n) \land 1 < d < n$	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: $a \mid b \wedge b \mid c \to a \mid c$

Proof:

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

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

Proof:

Assume: $p \in \mathbb{P}$	
$p = 1p$	Identity of Multiplication
Conclude: $p \mid p$	Definition of divides □
Otherwise: $p \notin \mathbb{P}$	
Follow this algorithm:	
Initial step:	
$p = a_1 b_1 \wedge 1 < a_1, b_1 < p$ 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: $a_1 \notin \mathbb{P}$	
$a_1 = a_2 b_2 \wedge 1 < a_2 < a_1 < p$	Definition of composite
Repeat with $a_1 \leftarrow a_2$	
***i*th step**	
$a_i = a_{i+1} b_{i+2} \wedge 1 < a_i < a_{i-1} < \underbrace{\dots}_{i \text{ times}} < p$	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:	
$a_{n-1} = a_n b_n \wedge 1 < a_n < \underbrace{\dots}_{p \text{ times}} < p$	
There can not be p unique numbers between 1 and p	
Therefore this process must terminate (call that place a_j)	Algorithm halts
$a_j \in \mathbb{P} \wedge a_j \mid a_{j-1} \wedge a_{j-1} \mid a_{j-2} \wedge \cdots \wedge a_1 \mid p$	Condition for termination
$a_j \in \mathbb{P} \wedge a_j \mid p$	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: $n \in \mathbb{P} \leftrightarrow \neg\exists p(p \in \mathbb{P} \wedge 1 < p \leq \sqrt{n} \wedge p \mid n)$

I will simply prove the biconditional with both sides negated.

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

Proof:

$\rightarrow$	
$n \notin \mathbb{P}$	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) ∎

Proof:

$\leftarrow$	
$p \in \mathbb{P} \wedge 1 < p \leq \sqrt{n} \wedge p \mid n$	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 ∎

2.4 $101 < 121$

$\sqrt{101} < \sqrt{121}$ since they are all positive

$\sqrt{101} < 11$

$\{p \mid p \in \mathbb{P} \wedge p < 11\} = \{2, 3, 5, 7\}$

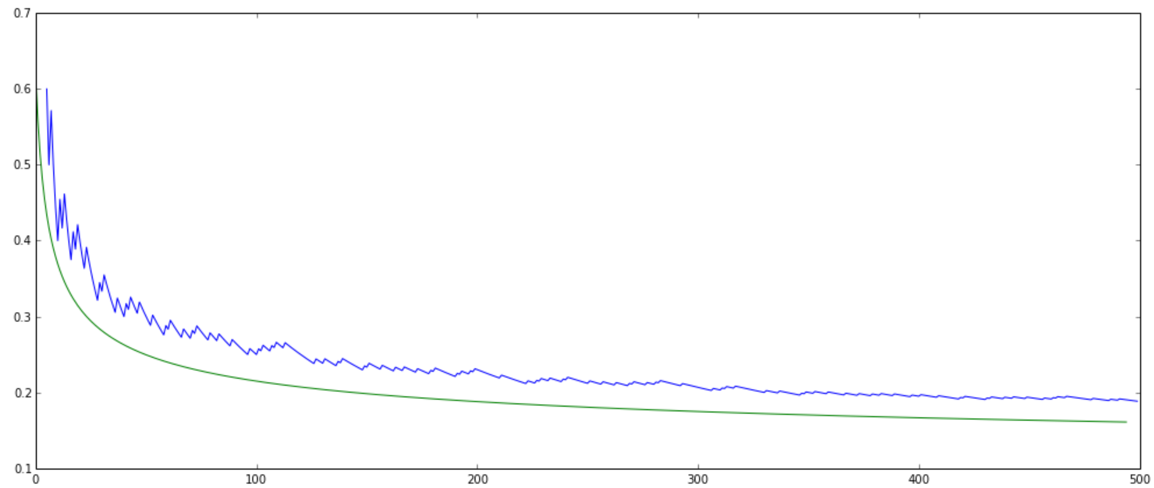
$2 \nmid 101 \wedge 3 \nmid 101 \wedge 5 \nmid 101 \wedge 7 \nmid 101$

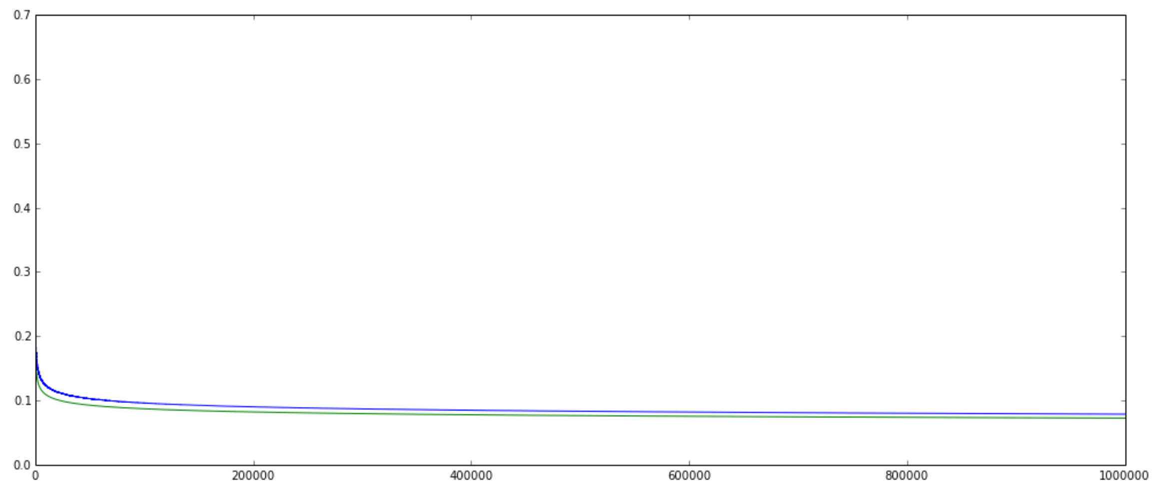
$\therefore 101 \in \mathbb{P}$

2.5

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

The green line is $\frac{1}{\ln(x)}$





2.7 Theorem: Every natural number n excluding one can be written as the product of primes $\{p_1, p_2, \ldots, p_m\}$ (not necessarily all unique). (In other words $n = p_1 p_2 \ldots p_m$.)

Proof:

$n \in \mathbb{N} \land n \neq 1$	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 $\frac{n}{p_1 p_2 \ldots p_i} = 1$:	
Conclude: $p_1 p_2 \ldots p_i = n$	
Otherwise: $\frac{n}{p_1 p_2 \ldots p_i} \neq 1$	
$\exists p_{i+1}(p_{i+1} \mid \frac{n}{p_1 p_2})$	Theorem 2.1
Result:	
Each iteration, n decreases.	
Therefore the algorithm halts.	
$p_1 p_2 \ldots p_m = n$	Halting condition $\blacksquare$

Note that I don't have exponents on the primes because I am letting them be necessarily unique. It is easier to prove this way.

2.8 Theorem: $pk = q_1 q_2 q_3 \ldots q_m n \wedge p \in \mathbb{P} \wedge \forall i(q_i \in \mathbb{P}) \rightarrow \exists i(p = q_i)$

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

Proof:

$p \in \mathbb{P} \wedge q \in \mathbb{P} \wedge p \neq q$	Premise
$\gcd(p, q) \mid p \wedge \gcd(p, q) \mid q$	Definition of GCD
$(a = 1 \vee a = q) \wedge (a = 1 \vee a = p)$	Definition of prime
$a = 1 \vee a = p = q$	Simplification
$p \neq q$	Premise
$a = 1$	Disjunctive syllogism $\blacksquare$

Proof:

$p \neq 1$	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
$\exists i\{q_i = p\}$	Quantifier Exchange ∎

2.9 Theorem: Every natural number excluding one has a **unique** prime factorization. Given a natural-number n greater than one, if $n = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_s$ then $\forall p_i \exists q_j (p_i = q_j) \land \forall q_j \exists p_i (p_i = q_j)$.

Proof:

$p_1p_2p_3p_4 \ldots p_m = q_1q_2q_3q_4 \ldots q_s$	Premise
$\exists i(p_1 = q_i) \land p_2p_3p_4 \ldots p_m = q_1q_2q_3q_4 \ldots q_{i-1}q_{i+1} \ldots q_s$	Lemma 2.8
$p_1 = q_1 \land p_2p_3p_4 \ldots p_m = q_2q_3q_4 \ldots q_s$	Reordering
	I am allowed to write the list in any order
	So I choose to write the matching q_i at the fro
$p_2 = q_2 \land p_3p_4 \ldots p_m = q_3q_4 \ldots q_s$	Lemma 2.8 (similar reordering)
$p_3 = q_3 \land p_4 \ldots p_m = q_4 \ldots q_s$	Lemma 2.8 (similar reordering)
$\vdots$	
$p_i = q_i$	By repetition
$m = s$	By repetition ∎

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 Theorem: $a \mid b \leftrightarrow \text{pf}(a) \subseteq \text{pf}(b)$

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

Proof:

$\rightarrow$

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

Proof:

$\leftarrow$

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

2.13 Theorem: $a^2|b^2 \to a|b$

Proof:

$a^2|b^2$ $\text{pf}(a^2) \subseteq \text{pf}(b^2)$	Division-subset theorem
$x\# \,\text{pf}(a^2) \leq x\# \,\text{pf}(b^2)$	Definition of subset-or-equal
$x\#(\text{pf}(a) + \text{pf}(a)) \leq x\#(\text{pf}(b) + \text{pf}(b))$	pf of product
$x\# \,\text{pf}(a) + x\# \,\text{pf}(a) \leq x\# \,\text{pf}(b) + x\# \,\text{pf}(b)$	pf of product
$2(x\# \,\text{pf}(a)) \leq 2(x\# \,\text{pf}(b))$	Algebra
$x\# \,\text{pf}(a) \leq x\# \,\text{pf}(b)$	Algebra
$\text{pf}(a) \subseteq \text{pf}(b)$	Definition of subset-or-equal
$a|b$	Division-subset theorem $\blacksquare$

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. Let us generalize this problem.

Lets assume I have a list of primes, but I need to do long-division to test for divisibility. In general, factoring a number assuming the $\pi(n) = \frac{n}{\ln(n)}$ as proposed in 2.6. This is in $\mathcal{O}(n)$ The number of steps in long-division is $\frac{n}{q}$. This is in $\mathcal{O}(n)$. In the worst case, I need to do the long division once for all $\pi(n)$ primes. Thus prime-factorizing can be done in $\mathcal{O}(n^2)$

On the other hand, we have the Euclidean Algorithm. Subtracting can be done digit-by-digit. It is in $\mathcal{O}(\log n)$ for this reason. 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. This runs in $\mathcal{O}(log(n))$ steps. Thus the Euclidean Algorithm as a whole runs in $\mathcal{O}(\log^2(n))$

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

2.18 Theorem: For any set of n numbers from 1 to $2n$, there exists a number that divides another number in that set.

Base Case:
If $n = 1$, the theorem is true,
since there is only one number to pick from.
Inductive Hypothesis:
The theorem holds for picking n numbers 1 to $2n$.
Assume it holds for picking all $k < n$ that picking n numbers less than or equal to $\{1, \ldots, 2k\}$.
Inductive Step:
Lets say we pick $n+1$ numbers less than or equal to $2(n+1)$.
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, $(n+1) \mid (2n+1)$
In the 3b case, construct a new set with $n-1$ numbers form $\{1, \ldots, 2n\}$ and $n+1$.
By the inductive hypothesis, There exists a number, call it j,
where $j \neq n+1 \wedge (j \mid (n+1) \vee (n+1) \mid j)$.
$(n+1) \mid j \wedge j \neq n+1 \rightarrow j \geq 2n+2$, but this is out of range for the list
Therefore $j \mid (n+1)$
$(n+1) \mid (2n+2)$, therefore $j \mid (2n+2)$
Therefore the theorem holds.

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

Proof:

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

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

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 can be absorbed into the n. But the three is 'left over'. 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 Theorem: $\sqrt{7} \notin \mathbb{Q}$

Proof:

$\sqrt{7} \in \mathbb{Q}$	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 Theorem: $\sqrt{12} \notin \mathbb{Q}$

Proof:

$\sqrt{12} \in \mathbb{Q}$	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
$32^2 n_0^2 n_1^2 n_2^2 \cdots = m_0^2 m_1^2 m_2^2 \ldots$	Substitution
$3n_0^2 n_1^2 n_2^2 \cdots = m_1^2 m_2^2 \ldots$	Theorem 2.8 (with reordering)
$3n_1^2 n_2^2 \cdots = m_2^2 \ldots$	Theorem 2.8 (with reordering)
$3n_1^2 n_2^2 \cdots = m_2^2 \ldots$	Theorem 2.8 (with reordering)
Continuing this process	
$3 = 1$	Theorem 2.8 (with reordering)
$\sqrt{12} \notin \mathbb{Q}$	Contradiction ■

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

Proof:

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

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

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

Proof:

$\sqrt[n]{x} \notin \mathbb{N}$	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
$xk_0^n k_1^n k_2^n \cdots = j_0^n j_1^n j_2^n \ldots$	FTA
$xk_1^n k_2^n \cdots = j_1^n j_2^n \ldots$	Theorem 2.8 (with reordering)
$xk_2^n \cdots = j_2^n \ldots$	Theorem 2.8 (with reordering)
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 ■

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

Proof:

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

$P \subseteq \mathrm{pf}(ab)$	Division-subset theorem
$P \subseteq A + B$	pf of product
$p\#P \leq p\#(A+B)$	Prime divisor theorem
$1 \leq p\#(A+B)$	Substitution
If: $p \mid a$	
Conclude: $p \mid a \vee p \mid b$	Addition □
Otherwise: $p \nmid a$	
$P \nsubseteq A$	Divisor-subset theorem
$\exists j \in [p](j\#P > j\#A)$	Definition of subset-or-equal (negated)
$p\#P > p\#A$	Quantifying over one element
$1 > p\#A$	Substition
$p\#A = 0$	Property of Natural numbers
$1 \leq p\#A + p\#B$	Definition of list-addition
$1 \leq p\#B$	Substition
$p\#P \leq p\#B$	Substitution
$\forall j \in [p](j\#P \leq j\#A)$	Quantifying over one element
$P \subseteq A$	Definition of subset-or-equal
$p \mid a$	Subset-divisor theorem
Conclude: $p \mid a \vee p \mid b$	Addition □
$p \mid a \vee p \mid b$	Either way (constructive dilemma) ■

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

Proof:

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

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

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

Proof:

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

$A \cap B = \{\}$	
$A \cap C = \{\}$	Coprime-disjoint theorem
$\gcd(a,bc) = A \cap (\mathrm{pf}(bc))$	GCD-intersection theorem
$= A \cap (B + C)$	pf of product
$= A \cap B + A \cap C$	Empty-intersection theorem
$= \{\} + \{\}$	Substitution
$= \{\}$	Identity
$\gcd(a,bc) = 1$	Coprime-disjoint theorem ■

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

Proof:

Let $x \in \mathbb{P}$

$x\#\,\mathrm{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) =$	
$= x\#(\mathrm{pf}(\frac{a}{\gcd(a,b)}) \cap \mathrm{pf}(\frac{b}{\gcd(a,b)}))$	GCD-intersection theorem
$= x\#(\mathrm{pf}(a) - \mathrm{pf}(\gcd(a,b))) \cap (\mathrm{pf}(b) - \mathrm{pf}(\gcd(a,b)))$	pf of fraction
$= x\#(\mathrm{pf}(a) - \mathrm{pf}(a) \cap \mathrm{pf}(b)) \cap (\mathrm{pf}(b) - \mathrm{pf}(a) \cap \mathrm{pf}(b))$	GCD-intersection theorem
$= \min(x\#\,\mathrm{pf}(a) - x\#(\mathrm{pf}(a) \cap \mathrm{pf}(b)), x\#\,\mathrm{pf}(b) - x\#(\mathrm{pf}(a) \cap \mathrm{pf}(b)))$	Definition of intersection
$= \min(x\#\,\mathrm{pf}(a) - x\#(\mathrm{pf}(a) \cap \mathrm{pf}(b)), x\#\,\mathrm{pf}(b) - x\#(\mathrm{pf}(a) \cap \mathrm{pf}(b)))$	Definition of list subtraction
$= \min(x\#\,\mathrm{pf}(a) - \min(x\#\,\mathrm{pf}(a), x\#\,\mathrm{pf}(b)),$ $x\#\,\mathrm{pf}(b) - \min(x\#\,\mathrm{pf}(a), x\#\,\mathrm{pf}(b)))$	Definition of intersection
Assume $\min(x\#pf(a), x\#\,\mathrm{pf}(b) = x\#\,\mathrm{pf}(a))$	
$= \min(x\#\,\mathrm{pf}(a) - x\#\,\mathrm{pf}(a), x\#\,\mathrm{pf}(b) - x\#\,\mathrm{pf}(a))$	Assumption

$= \min(0, x\#\,\mathrm{pf}(b) - x\#\,\mathrm{pf}(a))$ Algebra
$= 0$ Definition of min
Conclude $x\#\,\mathrm{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$
Otherwise $\min x\#pf(a), x\#\,\mathrm{pf}(b) = x\#\,\mathrm{pf}(b)$
$= \min(x\#\,\mathrm{pf}(a) - x\#\,\mathrm{pf}(b), x\#\,\mathrm{pf}(b) - x\#\,\mathrm{pf}(b))$ Assumption
$= \min(x\#\,\mathrm{pf}(a) - x\#\,\mathrm{pf}(b)), 0$ Algebra
$= 0$ Definition of min
Conclude $x\#\,\mathrm{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$
$x\#\,\mathrm{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = 0$ Either way
$\mathrm{pf}(\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})) = \{\}$ Notation for list
$\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$ Coprime-disjoint theorem ■

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

Proof:

Let $\mathrm{pf}(u) = U, \mathrm{pf}(v) = V, \mathrm{pf}(a) = A, \mathrm{pf}(b) = B$
$U \subseteq A$
$V \subseteq B$ 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 Theorem: $\forall n \in \mathbb{N}(\gcd(n, n+1) = 1)$

Proof:

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

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

Proof:

$\rightarrow$

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

Proof:

$\leftarrow$

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

Proof:

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

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

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

Proof:

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 Theorem: 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 Theorem: $\forall i (r_i \equiv 1 \pmod 4) \to r_1 r_2 \ldots r_m \equiv 1 \pmod 4$

Proof:

Let $i = 2$	**Base case**
$r_1 r_2 \equiv 1 \pmod 4$	Theorem 1.14
Let $r_1 r_2 \ldots r_{m-1} \equiv 1 \pmod 4$	**Inductive Hypothesis**
$(r_1 r_2 \ldots r_{m-1}) r_m \equiv 1 \pmod 4$	Theorem 1.14
$r_1 r_2 \ldots r_m \equiv 1 \pmod 4$	**Inductive Step** ∎

2.38 Theorem: There are an infinite number of primes, p, where $p \equiv 1 \pmod 4$

Lemma: All primes are odd except for two.

Proof:

Assume there is an even prime that isn't two.	
$p \in \mathbb{P} \land p \neq 2 \land p = 2n$ for some n	Assume for contradiction

$n \mid p$	Definition of divides
$p \notin \mathbb{P}$	Definition of prime $\neg\exists(p \in \mathbb{P} \wedge p \neq 2 \wedge p = 2n$ for son
$\forall p \in \mathbb{P}(p = 2 \vee p = 2n+1$ for some $n)$	Contradiction ■

All statements with $\equiv$ are assumed to be taken mod 4.

Proof:

Assume: p_k is the greatest prime where $p_k \equiv 3$	For contradiction
$\forall i(p_i = 2 \vee p_i = 2j+1$ for some $j)$	Lemma
$\forall i(p_i = 2 \vee p_i = 4j+1 \vee p_i = 4j+3$ for some $j)$	Algebra
$\forall i(p_i \equiv 2 \vee p_i \equiv 1 \vee p_i \equiv 3)$	Algebra
$\prod_{i=1}^{k} p_i \equiv 21^m 3^n$	Substitution
If: $n = 2j$ for some j (n is even)	
$\prod_{i=1}^{k} p_i \equiv 2 \cdot 1^m (3^2)^j$	Algebra
$\prod_{i=1}^{k} p_i \equiv 2 \cdot 1^m 1^j$	Substitution
$\prod_{i=1}^{k} p_i \equiv 2 \cdot 1^{m+j}$	Substitution
Conclude: $\prod_{i=1}^{k} p_i \equiv 2$	Substitution
Otherwise: $n = 2j+1$	
$\prod_{i=1}^{k} p_i \equiv 2 \cdot 1^m (3^2)^j 3$	Algebra
$\prod_{i=1}^{k} p_i \equiv 2 \cdot 3$	Algebra and Substitution
Conclude: $\prod_{i=1}^{k} p_i \equiv 2$	Algebra
$\prod_{i=1}^{k} p_i \equiv 2$	Either way
$1 + \prod_{i=1}^{k} p_i \equiv 3$	Substitution
$\forall i(p_i \nmid (1 + \prod_{i=1}^{k}))$	Same reasoning as 2.33
If: $\exists n(n \equiv 3 \wedge n \mid (1 + \prod_{i=1}^{k}))$	
Conclude: theorem holds	
Otherwise: $\neg\exists n(n \equiv 3 \wedge \mid (1 + \prod_{i=1}^{k}))$	
$\forall n(n \equiv 3 \rightarrow n \nmid (1 + \prod_{i=1}^{k}))$	Quantifier exchange, DeMorgan's, Conditional Disjunction, Contrapositive

$\prod_{i=1}^{k} p_i \equiv 2 \cdot 1^m 3^n \equiv 2 \cdot 1^m$ Prime factorization

$\prod_{i=1}^{k} p_i \equiv 2$ Substitution

That contradicts: $\prod_{i=1}^{k} p_i \equiv 2$

This branch of the conditional is impossible

■

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. Source: `http://primerecords.dk/aprecords.htm`

2.41 Theorem: $(x-1) \mid (x^n - 1)$

$$
\begin{array}{r|l}
 & x^{n-1} + x^{n-2} + x^{n-3} + x^{n-4} \ldots \quad +1 \\
\hline
x-1 & x^n \qquad\qquad\qquad\qquad\qquad -1 \\
 & -x^n + x^{n-1} \\
 & \quad -x^{n-1} + x^{n-2} \\
 & \qquad -x^{n-2} + x^{n-3} \\
 & \qquad\qquad \ddots \\
 & \qquad\qquad\qquad -x + 1
\end{array}
$$

2.42 Theorem: $2^p - 1 \in \mathbb{P} \to p \in \mathbb{P}$

Proof:

Assume $p \notin \mathbb{P}$	For conditional
$p = ab$	Definition of composite
$(2^a - 1) \vert (2^{ab} - 1)$	Theorem 1.41
Conclude: $2^p - 1 \notin \mathbb{P}$	Definition of composite
$p \notin \mathbb{P} \to 2^p - 1 \notin \mathbb{P}$	Conditional
$2^p - 1 \in \mathbb{P} \to p \in \mathbb{P}$	Contrapositive ■

2.43 Theorem: $2^p \in \mathbb{P} \to p = 2^n$ for some n

Proof:

Assume: $p \neq 2^n$ for some n	For conditional
$p = 2^n j$ for some $j \ni j$ is odd	FTA
$2^{2^n} \vert 2^{2^n j}$	Polynomial long division
Conclude: $2^{2^n j} \notin \mathbb{P}$	Definition of composite
$p \neq 2^n$ for some $n \to 2^{2^n j} \notin \mathbb{P}$	Conditional
$2^p \in \mathbb{P} \to p = 2^n$ for some n	Contrapositive ■

2.44 Theorem: there exists arbitrarily long (k-long) consecutive strings of composite integers.

Proof:

Let i be any number where $1 < i \leq k$	Let
$k! + i = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (i-1) \cdot i \cdot (i+1) \cdot \ldots k + i$	Definition of factorial
$= i \cdot (1 \cdot 2 \cdot 3 \cdot \cdots \cdot (i-1) \cdot (i+1) \cdot \ \ldots k + 1)$	distributive property
$i \vert (k! + i)$	Definition of divides
$i \neq 1$	Premise for i
$(k! + i) \not\in \mathbb{P}$	Definition of composite $\blacksquare$