Sam Grayson's Notebook (with LaTeX)

February 24, 2015

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

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
$\neg \exists a, b \in \mathbb{N} (p = ab \land 1 < a, b < p)$	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
$p = ab \rightarrow \neg (1 < a < p)$	Conditional disjunction
$p = ab \rightarrow \neg 1 < a \land a < p$	Property of inequality
$p = ab \rightarrow \neg (1 < a) \lor \neg (a < p)$	DeMorgan's law
$p = ab \rightarrow 1 \geq a \lor a \geq p$	Property of inequality
$p = ab \rightarrow (1 = a \land a \geq p)$	Property of Natural numbers
$p = ab \rightarrow (1 = a \land a = p)$	$a \| p \rightarrow a \leq p$
$a \| p \rightarrow (1 = a \land a = p)$	Definition of division
$\forall a (a \| p \rightarrow (1 = a \lor a = p))$	Universal generalization
p is prime	Definition of primes ■

$p \in \mathbb{P}$	Premise
$\neg (\forall d (d \| n \rightarrow (d = 1 \lor d = n)))$	Definition of prime
$\exists d \neg (d \| n \rightarrow (d = 1 \lor d = n))$	Quantifier exchange
$\exists d \neg (\neg (d \| n) \lor (d = 1 \lor d = n))$	Conditional disjunction
$\exists d \neg \neg (d \| n) \land \neg (d = 1 \lor d = n)$	DeMorgan's law
$\exists d d \| n \land \neg (d = 1 \lor d = n)$	Double Negation
$\exists d d \| n \land \neg d = 1 \land \neg d = n$	DeMorgan's law
$\exists d d \| n \land 1 < d < n$	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: $a | b \land b | c \rightarrow a | c$

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

Theorem: $n \in \mathbb{N} \land n \neq 1 \to \exists p(p \in \mathbb{P} \land p \mid n)$	
If $p \in \mathbb{P}$	
$p = 1p$	Identity of Multiplication
$p \mid p$	Definition of divides $\square$
Otherwise, $p \notin \mathbb{P}$	
Follow this algorithm:	
$p = a_1 b_1 \land 1 < a_1, b_1 < p$ 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
$\vdots$	
$a_i = a_{i+1} b_{i+2} \land 1 < a_i < a_{i-1} < \underbrace{\ldots}_{i \text{ times}} < p$	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	
$\vdots$	
$a_{n-1} = a_n b_n \land 1 < a_n < \underbrace{\ldots}_{p \text{ times}} < p$	
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 $\blacksquare$

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
$\neg(a > \sqrt{n}) \lor \neg(b > \sqrt{n})$	Contradiction
$a \leq \sqrt{n} \lor b \leq \sqrt{n}$	Property of inequality

Either way:

$\exists p(1 < p \leq \sqrt{n} \in \mathbb{N})$	Existential instantiation (on a or on b) $\blacksquare$

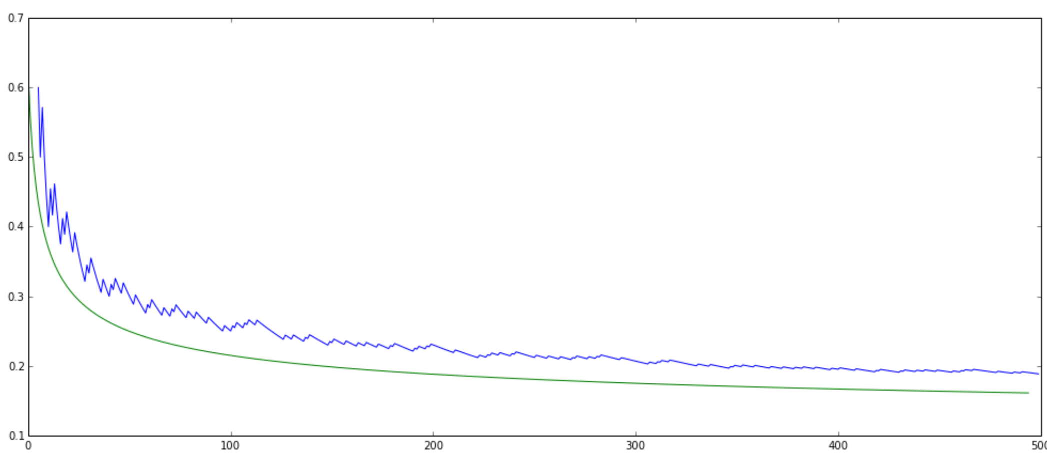
$\leftarrow$

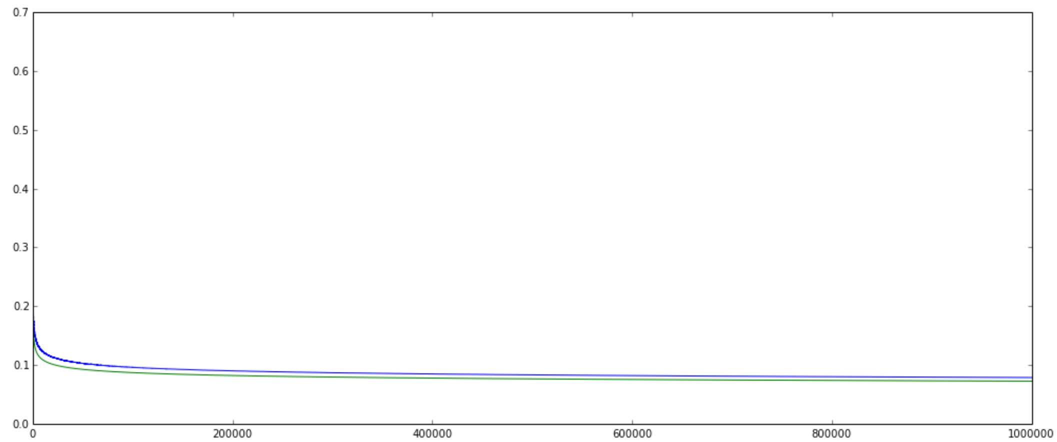
$p \in \mathbb{P} \wedge 1 < p \leq \sqrt{n} \wedge p \mid n$	Universal instantiation
$\sqrt{n} < n$	Property of positive numbers
$1 < p < n$	Property of inequalities
$\exists c(1 < c < n \wedge pc = n)$	Definition of divides
$1 < p, c < n \wedge pc = n$	Restatement
$n \notin \mathbb{P}$	Definition of 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 excluding one has a prime factorization.

$\forall_{n\in\mathbb{N}\setminus\{1\}}(\exists_{\{p_1,p_2,\ldots,p_n\}\subset\mathbb{P}}\ \exists_{\{r_1,r_2,\ldots r_3\}\subset\mathbb{N}}(\prod^{i} p_i^{r_i} = n))$

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

$(p,q)\|p \wedge (p,q)\|q$	Definition of GCD
$(a = 1 \vee a = q) \wedge (a = 1 \vee a = p)$	Definition of prime
$p \neq q$	Premise
$a = 1 \vee a = p = q$	Simplification
$a = 1$	Disjunctive syllogism ■

$p \neq \|1$	Premise
$p\|(\prod_{i=1}^{n} q_i)$	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)
$p\|q_1 \prod_{i=2}^{n} q_i$	Algebra
$(p, q_1) = 1$	Coprime primes lemma
$p\| \prod_{i=2}^{n} q_i$	Theorem 1.41 (Base case)
$p\| \prod_{i=j}^{n} q_i$	Assume (Inductive hypothesis)
$p\|q_{j+1} \prod_{i=j+1}^{n} q_j$	Algebra
$(p, q_j) = 1$	Coprime primes lemma
$p\| \prod_{i=j+1}^{n}$	Theorem 1.41 (Inductive Step)
$p\| \prod_{i=n}^{n}$	Inductive axiom
$p\|1 \wedge p\neg\|1$	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 $2^{12+5+3+1}$
$5^{5+1}\cdot 2^{12+5+3+1}|25$
$5^6\cdot 2^{21}|25$
$10^6\cdot 2^{21-6}|25$
The largest power of 10 that divides 25 is 10^6
There are 6 zeros at the end of 25!

2.12

$a|b \leftrightarrow \mathrm{pf}(a) \subseteq \mathrm{pf}(b)$	Premise
$ma = b$ for some $m \in \mathbb{Z}$	Definition of divides
$\mathrm{pf}(ma) = \mathrm{pf}(b)$ for some $m \in \mathbb{Z}$	pf is injective
$\mathrm{pf}(m) + \mathrm{pf}(a) = \mathrm{pf}(b)$	pf of product theorem
$\mathrm{pf}(a) \subseteq \mathrm{pf}(b)$	addend-subset theorem ∎

2.13

$a^2|b^2 \leftrightarrow a|b$	Premise
$a = p_1^{r_1}p_2^{r_2}\ldots$	
$b = q_1^{t_1}q_2^{t_2}\ldots$	Fundamental Theorem of Rithmetic
$a^2 = p_1^{2r_1}p_2^{2r_2}\ldots$	
$b^2 = q_1^{2t_1}q_2^{2t_2}\ldots$	Algebra
$\mathrm{pf}(a) \subset \mathrm{pf}(b)$	I don't know

∎

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

2.16 $\gcd(a,b) = \mathrm{pf}(a)\cap\mathrm{pf}(b)$
$\mathrm{lcm}(a,b) = \mathrm{pf}(a)\cup\mathrm{pf}(b)$

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 $\int_{x=1}^{x=n} \frac{1}{\ln(x)}\,dx = n\ln(n) - n - 1$. 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 ∞.

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 $\{1, \dots 2n\}$ (**Inductive Hypothesis**)
Lets say we pick $n + 1$ numbers less than or equal to $2(n + 1)$
We pick from $1 to 2n + 2$
We pick from $\{1, \dots, 2n, 2n + 1, 2n + 2\}$

2.18 There are three options:
First, we can pick $n + 1$ numbers from $\{1, \dots, 2n$
Second, we can pick n numbers from $\{1, \dots, 2n\}$ and 1 number from $\{2n + 1, 2n + 2\}$
Third, we can pick $n - 1$ numbers from $\{1, \dots, 2n\}$ 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, the

2.24 Let $n \in \mathbb{Q}$ and $x \in \mathbb{N}$. $x^n \in \mathbb{N} \vee x^n \notin \mathbb{Q}$

2.28 $(b, c) = 1 \rightarrow (a, bc) = (a, b) \cdot (a, c)$
$a = \prod A$ where $A \subset \mathbb{P}$
$b = \prod B$ where $B \subset \mathbb{P}$
$c = \prod C$ where $C \subset \mathbb{P}$ Fundamental theorem
$B \cap C = \emptyset$ $\blacksquare$