Test 2

Sam Grayson

March 30, 2015

Before beginning the my answers, I need to establish the following lemma.
Lemma: $\forall i \in \mathbb{N}(\forall j \in \mathbb{N}(\exists! r \in \mathbb{N}(i \equiv r \pmod{j} \wedge 0 \leq r < j)))$
Proof:

Let $i \in \mathbb{N}$	(for universal generalization)
Let $j \in \mathbb{N}$	(for universal generalization)
$i = qj + r \wedge 0 \leq r < j$ for some unique $q, r \in \mathbb{N}$	Division algorithm
$i - r = qj$	Algebra
$j \mid (i - r)$	Definition of divides
$i \equiv r \pmod{j}$	Definition of modulo
$i \equiv r \pmod{j} \wedge 0 \leq r < j$	Conjunction
$\exists r(i \equiv r \pmod{j} \wedge 0 \leq r < j)$	Existential generalization
$\forall i \in \mathbb{N}(\forall j \in \mathbb{N}(\exists! r \in \mathbb{N}(i \equiv r \pmod{j} \wedge 0 \leq r < j)))$	Universal generalization ■

1. **Theorem:** $\sqrt[3]{6} \notin \mathbb{Q}$

   Proof:

$\sqrt[3]{6} \neq 1$	Fact
$\sqrt[3]{6} \neq 2$	Fact
$\sqrt[3]{6} \neq 3$	Fact
$\sqrt[3]{6} \neq 4$	Fact
$\sqrt[3]{6} \neq 5$	Fact
$\sqrt[3]{6} \neq 6$	Fact
$\forall x \in \mathbb{N}(1 \leq \sqrt[3]{x} \leq x)$	Fact
$1 \leq \sqrt[3]{6} \leq 6$	Universal instantiation
Ugggggh	
$\sqrt[3]{6} \notin \mathbb{N}$	By exhaustion
$\sqrt[3]{6} \notin \mathbb{Q}$	Next test question ■

2. **Theorem:** Let $n, x \in \mathbb{N}$. $\sqrt[n]{x} \in \mathbb{Q} \rightarrow \sqrt[n]{x} \in \mathbb{N}$.

   Proof:

$\sqrt[n]{x} \in \mathbb{Q}$	Premise
$\sqrt[n]{x} = \frac{j}{k}$ 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 (with reordering)
$xk_2^n \ldots = j_2^n \ldots$	Theorem 2.8 (with reordering)
Repeating this process	

Stop when all k are eliminated
Lets call it the ith step

$x = j_i^n j_{i+1}^n \dots$	Theorem 2.8
$\sqrt[n]{x} = j_i j_{i+1} \dots$	Algebra
$\sqrt[n]{x} \in \mathbb{N}$	Closure of $\mathbb{N}$ over multiplication ∎

3. **Theorem:**: Let $n \equiv 2 \pmod 3$. Let the prime-factorization of n be written as follows: $n = n_1 n_2 n_3 \dots$. I claim that $\exists i(n_i \equiv 2)$

Proof:

Note: all statements of congruency are taken to be modulo 3.

Assume $\forall i(n_i \not\equiv 2)$	For contradiction
$\forall i(i \equiv 0 \vee i \equiv 1 \vee i \equiv 2))$	Lemma
$\forall i(i \not\equiv 2 \to (i \equiv 2 \vee i \equiv 0))$	Conditional disjunction
$n_i \not\equiv 2$	Universal instantiation
$n_i \not\equiv 2 \to (n_i \equiv 1 \vee n_i \equiv 0)$	Universal instantiation
$n_i \equiv 1 \vee n_i \equiv 0$	Modus ponens
$\forall i(n_i \equiv 1 \vee n_1 \equiv 0)$	Universal generalization
$n_0 n_1 n_2 \dots \equiv 1^i 0^j$ for some $i, j \in \mathbb{N}$	Theorem 1.14 (repeated use)
If $i = 0 \wedge j \neq 0$: $n \equiv 0$	Arithmetic
If $i \neq 0 \wedge j = 0$: $n \equiv 1$	Arithmetic
If $i \neq 0 \wedge j \neq 0$: $n \equiv 0$	Arithmetic
If $i = 0 \wedge j = 0$: $n \equiv 1$	Arithmetic
$n \equiv 0 \vee n \equiv 1$	Constructive dilemma
Contradicts $n \equiv 2$	
$\neg(\forall i(n_i \not\equiv 2))$	Contradiction
$\neg(\neg\exists i(n_i \equiv 2))$	Quantifier exchange
$\exists i(n_i \equiv 2)$	Double negation ∎

4. (a) Theroem: $(a \in H \wedge b \in H) \to ab \in H$.

Proof:

$a = 4c + 1$	Definition of Hilbert number
$b = 4d + 1$	Definition of Hilbert number
$ab = 16cd + 4c + 4d + 1 = 4(4cd + c + d) + 1$	Algebra
$ab \equiv 1 \pmod 4$	Definition of modulo
$ab \in H$	Definition of H ∎

(b) 5, 9, 13, 17, 21, 29, 33, 37, 41, 49

(c) Show: for all $a \in H$, a can be factored into elements of H

Some Hilbert numbers a are divisible by some other Hilbert element $b \in H$. In order for a to factor, it has to be written as $a = bc$ for $c \in H$. In other words, $\forall a \in H(\forall b \in H(b|a \to \exists c \in H(bc = a)))$. (These are the Hilbert composites)

Proof:

Note: all statements of congruency are taken to be modulo 4.

Let $a \in H$	Assume (for universal generalization)
Let $b \in H$	Assume (for universal generalization)
Let $b\|a$	Assume (for conditional)
$bc = a$ for some $c \in \mathbb{N}$	Definition of divides and existential instantiation (on c)
$a = 4k_a + 1$ for some k_a	Definition of Hilbert number
$b = 4k_b + 1$ for some k_b	Definition of Hilbert number
$a - 1 = 4k_a$	Algebra
$b - 1 - 4k_b$	Algebra
$4\|(a-1)$	Definition of divides
$4\|(b-1)$	Definition of divides
$a \equiv 1$	Definition of modulo
$b \equiv 1$	Definition of modulo
$\forall i(i \equiv 0 \vee i \equiv 1 \vee i \equiv 2 \vee i \equiv 3)$	Lemma
Assume $c \not\equiv 1$	For contradiction
$i \equiv 0 \vee i \equiv 1 \vee i \equiv 2 \vee i \equiv 3$	Universal instantiation
$c \not\equiv 1 \rightarrow (c \equiv 0 \vee c \equiv 2 \vee c \equiv 3)$	Universal generalization
$i \not\equiv 1 \rightarrow (i \equiv 0 \vee i \equiv 2 \vee i \equiv 3)$	Conditional disjunction
$c \equiv 0 \vee c \equiv 2 \vee c \equiv 3$	Modus ponens
If $c \equiv 0$: $bc \equiv 1 \cdot 0 \equiv 0$	Theorem 1.14
If $c \equiv 2$: $bc \equiv 1 \cdot 2 \equiv 2$	Theorem 1.14
If $c \equiv 3$: $bc \equiv 1 \cdot 3 \equiv 3$	Theorem 1.14
$bc \equiv 0 \vee bc \equiv 2 \vee bc \equiv 3$	Constructive dilemma
Contradicts $bc \equiv 1$	
$c \equiv 1$	Contradiction
$c \in H$	Definition of Hilbert number
$\exists c \in H(bc = a)$	Existential generalization
$b\|a \rightarrow \exists c \in H(bc = a)$	Conditional proof
$\forall b \in H(b\|a \rightarrow \exists c \in H(bc = a))$	Universal generalization
$\forall a \in H \forall b \in H(b\|a \rightarrow \exists c \in H(bc = a))$	Universal generalization ■

Every Hilbert number that is not divisible by another Hilbert number can be written $a = 1a$, since $1 \in H$ and $a \in H$. (These are the Hilbert primes).

Therefore every Hilbert number can be factored into other Hilbert numbers,

(d) $693 = 9 \cdot 77$
$693 = 21 \cdot 33$

5. (a) Using finite-list notation, the GCD is equivalent to the list-intersection. Since 3 occurs in the prime-factorization of a 3 times and in the prime-factorization of b 2 times, 3 occurs in the prime factorization of the GCD $\min(3, 2) = 2$.

$A = \text{pf}(a) = \{2, 2, 2, 3, 3, 5, 5, 13\}$
$B = \text{pf}(b) = \{2, 2, 3, 3, 3, 13, 13, 13, 13, 13, 13, 13, 19\}$
$\min(2\#A, 2\#B) = \min(3, 2) = 2$
$\min(3\#A, 3\#B) = \min(2, 3) = 2$
$\min(13\#A, 13\#B) = \min(1, 7) = 1$
$\text{pf}(a) \cap \text{pf}(b) = \{2, 2, 3, 3, 13\}$
$\gcd(a, b) = \prod(\text{pf}(a) \cap \text{pf}(b)) = 156$

(b) $A = \text{pf}(a) = \{2, 2, 2, 3, 3, 5, 5, 13\}$
$B = \text{pf}(b) = \{2, 2, 3, 3, 3, 13, 13, 13, 13, 13, 13, 13, 19\}$
$\text{pf}(6a^2 + 5b^3) = \{2, 3\} + 2A + \{5\} + 3B$
$2\#\,\text{pf}(6a^2 + 5b^3) = 2\#(\{2, 3\} + 2A + \{5\} + 3B)$
$= 1 + 2 \cdot 3 + 0 + 3 \cdot 2$
$= 13$
$2^13 \mid (6a^2 + 5b^3)$

6. **Theorem:** Let $n \in \mathbb{Z} \wedge n > 0$. Let the smallest prime factor be p. $p > \sqrt[3]{n} \to (\frac{n}{p} = 1 \vee \frac{n}{p} \in \mathbb{P})$

Consider the case where n is composite. $\frac{n}{p} \in \mathbb{P}$. Therefore, the theorem holds.

Proof:

Assume $p > \sqrt[3]{n}$ is the smallest prime factor	For conditional
$\frac{1}{p} < \frac{1}{\sqrt[3]{n}}$	Property of inequality
$\frac{n}{p} < \frac{n}{\sqrt[3]{n}}$	Property of inequality
$\frac{n}{p} < n^{2/3}$	Property of inequality
$n \neq p$	A prime cannot equal a composite
$\frac{n}{p} \neq 1$	Algbera
Assume $\frac{n}{p} \notin \mathbb{P}$	For contradiction
$\frac{n}{p} \in \mathbb{P} \leftrightarrow \neg\exists p(p \in \mathbb{P} \wedge 1 < p \leq \sqrt{\frac{n}{p}} \wedge p \mid \frac{n}{p})$	Theorem 2.3
$\frac{n}{p} \notin \mathbb{P} \leftrightarrow \exists j(j \in \mathbb{P} \wedge 1 < j \leq \sqrt{\frac{n}{p}} \wedge j \mid \frac{n}{p})$	Negative biconditional
$\exists j(j \in \mathbb{P} \wedge 1 < j \leq \sqrt{\frac{n}{p}} \wedge j \mid \frac{n}{p})$	Modus Ponens (on biconditional)
$j \in \mathbb{P} \wedge 1 < j \leq \sqrt{\frac{n}{p}} \wedge j \mid \frac{n}{p}$	Existential instantiation
$j \leq \sqrt{\frac{n}{p}}$	Simplification
$j \leq n^{1/3}$	Algebra
$j \mid \frac{n}{p}$	Simplification
$j \mid p\frac{n}{p}$	Theorem 1.3
$j \mid n$	Algebra
$j \leq p \wedge j \mid n \wedge j \in \mathbb{P}$	Conjunction
Contradicts premise for p	
Since j is a smaller prime factor	
$\frac{n}{p} \in \mathbb{P}$	Contradiction ∎

Consider the case where $n \in \mathbb{P}$. The smallest prime factor p is itself n. $\frac{n}{p} = 1$ (since both non-zero by premises). Therefore, theorem holds.

Consider the case where $n = 1$. Actually, don't consider the case where $n = 1$. There are no prime factors of one, so the antecedant is false. The theorem holds.

The theorem holds when $n \in \not{\mathbb{P}}$, $n \in \mathbb{P}$, and $n = 1$. These are the only three possibilities for positive integers.

7. **Algorithm:** Input $n \in \mathbb{N} \wedge n > 11$. Output two numbers $a \in \not{\mathbb{P}}$, and $b \in \not{\mathbb{P}}$ where $a + b = n$

Proof:

If $n \equiv 0 \pmod 2$	
$2 \mid n$	Definition of modulo
$n > 11$	Premise
$n - 4 > 7$	Property of inequalities
$n - 4 \neq 2$	Property of inequalities
$2 \vert (n-4)$	Theorem 1.2
$(n-4) \in \not{\mathbb{P}}$	Definition of composite
$4 = 2 \cdot 2$	
$\exists j(1 < j < 4 \wedge j \vert 4)$	Existential generalization
$4 \in \not{\mathbb{P}}$	Definition of composite
$(n-4) + 4 = n$	Algebra
Output $(n-4)$ and 4	
Otherwise $n \not\equiv 0 \pmod 2$	
$\forall i(i \equiv 0 \pmod 2 \vee i \equiv 1 \pmod 2)$	Lemma
$n \equiv 0 \pmod 2 \vee n \equiv 1 \pmod 2$	Universal instantiation
$n \not\equiv 0 \pmod 2 \to n \equiv 1 \pmod 2$ $n \equiv 1 \pmod 2$	Modus ponens
$n > 11$	Premise
$n - 9 > 9$	Premise
$2 \mid (9-1)$	
$9 \equiv 1 \pmod 2$	Definition of modulo
$n - 9 \equiv 1 - 1 \equiv 0 \pmod 2$	Theorem 1.13
$2 \mid (n-9)$	Definition of modulo
$n \neq 11$	Simplification
$n - 9 \neq 2$	Property of inequality
$n - 9 \in \not{\mathbb{P}}$	Definition of composite
$9 = 3 \cdot 3$	
$\exists j(1 < j < 9 \wedge j \vert 9)$	Existential generalization
$9 \in \not{\mathbb{P}}$	Definition of composite
$(n-9) + 9 = n$	Algebra
Output $n - 9$ and 9 $\blacksquare$	

8.

9. **Theorem:** Let n be a natural number greater than one. $\exists p \in \mathbb{P}(n \geq p \geq n! + 1)$.

Proof:

Let $m \in \mathbb{N} \wedge 1 < m < n$ (For universal generalization)

$n > 1$	Premise
$n! > 1$	Fact (given $n > 1$)
$\forall n \in \mathbb{N}(\gcd(n, n+1) = 1)$	Theorem 2.32
$\gcd(n!, n!+1) = 1$	Universal instantiation
Assume $m \vert (n!+1)$	For contradiction
$m \mid n!$	Definition of factorial since $m < n$
$\gcd(n, n+1) \geq m$	Definition of gcd
$\gcd(n, n+1) \geq m > 1$	Restatement (Premise for m)
$\gcd(n, n+1) > 1$	Property of inequalities
Therefore $m \nmid n!+1$	Lemma
$\forall m(1 < m < n \to m \nmid (n!+1))$	Universal generalization
$\exists p(p \in \mathbb{P} \wedge p \mid (n!+1))$	Fundamental Theorem of Arithmetic
Let $p \in \mathbb{P} \wedge p \mid (n!+1)$	Existential instantiation
$1 < p < n \to p \nmid (n!+1)$	Universal instantiation
$p \mid (n!+1) \to \neg(1 < p < n)$	Contrapositive
$p \mid (n!+1)$	Simplification
$\neg(1 < p < n)$	Modus ponens
$\neg(1 < p \wedge p < n)$	Modus ponens
$\neg(1 < p) \vee \neg(p < n)$	Modus ponens
$\neg(1 < p) \vee p \geq n$	Property of inequality
$\neg\neg(1 < p) \to p \geq n$	Conditional disjunction
$1 < p \to p \geq n$	Double negation
$1 < p$	p is prime
$p \geq n$	Modus ponens
$ap = (n!+1)$ for some $a \in \mathbb{N}$	Definition of divides and existential instantiation (on a)
$p \leq (n!+1)$	Property of inequality
$n \leq p \wedge p \leq (n!+1)$	Conjunction
$n \leq p \leq (n!+1)$	Property of inequalities
$\exists p \in \mathbb{P}(n \leq p \leq (n!+1))$	Existential quantification ■

10.