Московский физико-технический институт
Факультет инноваций и высоких технологий
Математическая логика и теория алгоритмов, весна 2012
Формальная арифметика

Язык арифметики содержит один константный символ 0, один одноместный функциональный символ S и двухместные функциональные символы $+$ и $\cdot$. Единственным (двухместным) предикатным символом языка является равенство.

В стандартной интерпретации переменные принимают значения в множестве натуральных чисел $\mathbb{N}$, символ 0 интерпретируется как ноль, S как операция прибавления единицы, а $+$ и $\cdot$ как сложение и умножение соответственно.

Формула в языке арифметики со свободными переменными задаёт некоторый предикат. Если предикат можно выразить некоторой формулой в языке арифметики, то он называется *арифметичным.* Например, свойство (одноместный предикат) «x чётно» арифметично, т.к. его можно выразить формулой $\exists y(x = y + y)$.

1. Выразите в арифметике следующий предикаты:

a) Свойство «x есть простое число» (ниже мы обозначаем эту формулу $\mathrm{Prime}(x)$);
b) Отношение (двухместный предикат) $x > y$;
c) Отношение «x делит y»;
d) Трёхместный предикат «m/n есть рациональное приближение числа $\sqrt{2}$ с точностью $1/k$ »;
e) Трёхместный предикат «z есть наибольший общий делитель x и y» (Ниже мы обозначаем эту формулу $\gcd(x, y, z)$.)
f) Свойство «x есть степень двойки»;
g) Свойство «x есть степень четверки».

Для доказательства арифметичности многих предикатов используется мощный инструмент, называемый β-функцией Гёделя.

2. Докажите, что для любого n найдётся такое b, что числа $b+1, \ldots, nb+1$ попарно взаимно просты. Более того, b может быть сколь угодно большим.

3. Докажите, что для любого набора $(x_1 \ldots, x_n)$ найдутся числа a и b, такие что $a \equiv x_i \mod (bi + 1)$ при всех i от 1 до n.

4. Докажите, что функция $\beta(a, b, i) = a \mod (bi + 1)$ арифметична. (Т.е. четырёхместный предикат «$x = \beta(a, b, i)$» арифметичен.)

5. Выразите на языке формальной арифметики следующие предикаты:

a) Свойство «x есть степень шестёрки»;
b) Двухместный предикат $x = 2^y$;
c) Двухместный предикат «x есть n-ое по счёту простое число»;
d) Двухместный предикат $x = n!$;
e) Свойство «x есть совершенное число»(т.е. оно равно сумме всех своих делителей, крмое самого себя);
f) Двухместный предикат «m есть целая часть числа e^x».

Система аксиом Пеано формальной арифметики состоит из 7 индивидуальных аксиом и одной бесконечной серии аксиом (эту серию аксиом называют *схемой индукции*)

- $\forall x(\neg(0 = Sx))$
- $\forall x\forall y(Sx = Sy \to x = y)$
- $\forall x(\neg(x = 0) \to \exists y(x = Sy))$
- $\forall x(x + 0 = x)$
- $\forall x\forall y(x + Sy = S(x + y))$
- $\forall x(x \cdot 0 = 0)$
- $\forall x\forall y(x \cdot (Sy) = (x \cdot y) + x)$
- $(\varphi(0)\&\forall x(\varphi(x) \to \varphi(Sx))) \to \forall x\varphi(x)$,

где $\varphi(x)$ произвольная формула со свободной переменной x.

В следующих задачах нужно доказать выводимость некоторых формул из аксиом Пеано.

6. PA $\vdash S(S0) + S(S0) = S(S(S(S0)))$.

7. PA $\vdash S(S0) \cdot S(S0) = S(S(S(S0)))$.

8. PA $\vdash \forall x(x \cdot S0 = x)$.

9. PA $\vdash \forall x(0 + x = x)$.

10. PA $\vdash \forall x(0 + x = x)$.

11. PA $\vdash \forall x\forall y(Sx + y = S(x + y))$.

12. PA $\vdash \forall x\forall y(x + y = y + x)$.

13. PA $\vdash \forall x(0 \cdot y = 0)$.

14. PA $\vdash \forall x\forall y((Sx) \cdot y = y \cdot x + x)$.

15. PA $\vdash \forall x\forall y(x \cdot y = y \cdot x)$.

16. PA $\vdash \forall x\forall y\forall z((x + y) + z = x + (y + z))$.

17. PA $\vdash \forall x\forall y\forall z(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$.

18. PA $\vdash \forall n(n > 1 \to \exists p\ ((p \mid n) \wedge \mathrm{Prime}(p)))$, где $\mathrm{Prime}(p)$ означает, что число p простое, а $p \mid n$ означает, что p делит n. Данная формула имеет простой содержательный смысл: у любого числа больше единицы существует простой делитель. (Из задачи 1 мы знаем, что отношения «n больше единицы», «p делит n» и «p есть простое число» можно выразить в арифметике).

19. PA $\vdash \forall n\exists m\ (m > n \wedge \mathrm{Prime}(m))$. (Т.е. существуют сколь угодно большие простые числа).

20. PA $\vdash \forall x\forall y((\neg x = 0 \wedge \neg y = 0) \to \exists z\ \mathrm{gcd}(x, y, z))$, где $\mathrm{gcd}(x, y, z)$ означает, что z равно наибольшему общему делителю x и y. (Т.е. у любых двух положительных целых чисел есть наибольший общий делитель).

21. Докажите, что из PA можно вывести любую истинную формулу из класса Σ_1.