Applied Number Theory: Homework 1

Joshua Dong

September 9, 2016

1.14

a)

b is positive and non-zero. If a is positive, we can choose $q = 0$, and a will be in the set and we are done.
If a is 0, we can choose $q = -1$, and $b = 0 - b(-1)$ which will be in the set and we are done.
If a is negative, then we can choose $q = a + 1$. Then $a - b(a - 1) = a - ab + b = a(1 - b) + b$. $b > 0$ implies $b - 1 > -1$, $1 - b < 1$. If $1 - b$ is zero, $a(1 - b) + b = a(0) + b = b$, which is positive. If $1 - b$ is negative (which is the only other case, since b is an integer), $a(1 - b)$ is positive since the product of two negative numbers is positive. The sum of two positive numbers is positive, so $a(1 - b) + b$ would be positive.
In all cases, there must be a positive element of the set.

b)

Consider the set of integer multiples of b less than or equal to a. Denote this new set A. By the well-ordering principle, there is a greatest element of the set. Let this element be xb, where x is an integer.
$a = xb + y$ for some $y \geq 0$. $(x + 1)b$ is not in the set A but is a multiple, so $(x + 1)b > a$. $(x + 1)b = xb + b > a = xb + y$. $xb + b > xb + y$. $b > y$.
Then there exists $0 \leq y < b$ for any integer choice of a and b.

c)

We already showed this in b) with the set of integer multiples. Simply take $q = x$, $r = y$.

d)

$a = bq_1 + r_1 = bq_2 + r_2$.
$bq_1 + r_1 = bq_2 + r_2$
$bq_1 - bq_2 = r_2 - r_1$
$b(q_1 - q_2) = r_2 - r_1$.
But this means the difference between r_1 and r_2 is divisible by b. We know the two remainders are greater than 0. If their difference was greater than 0, then their difference would be at least b (by the definition of divisibility, and since q is integral). This is a contradiction with the assumption that $r_{1,2} < b$.
Then their difference must be 0, the only remaining possibility. If the remainders are the same, then q_1 and q_2 must be the same by the assertion of their relation to a.

1.23

m is odd. a is an integer. First we show that squares of even integers are equal to 0 modulo 4, and squares of odd integers are equal to 1 modulo 4.
Let $2k$ be an even integer, for some integer k, by definition of even. Then $(2k)^2 = 4k^2 = 4(k^2)$ is equivalent to 0 modulo 4 by definiton of modulo. Let $2k + 1$ be an even integer, for some integer k, by definition of odd. Then $(2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$ is equivalent to 1 modulo 4 by definiton of modulo.
Since m is odd, by definition there exists some integer x such that $m = 2x + 1$. Then $2m + a^2 \equiv 2(2x + 1) + a^2 \equiv 4x + 2 + a^2 \equiv 2 + a^2 \mod 4$.
If a is even, we showed its square is equivalent to 0 modulo 4. Then $2 + a^2 \equiv 2 \mod 4$. This cannot be a square, as shown previously.
If a is odd, we showed its square is equivalent to 1 modulo 4. Then $2 + a^2 \equiv 3 \mod 4$. This cannot be a square, as shown previously.
Then any number in the form of $2m + a^2$ where m is odd can never be a perfect square.

1.25

This is the same algorithem I implemented for fast modular exponentiation. It works since we take the binary representation and multiply the exponents of those bases. The floor function is simply a bit shift, taking the next least significant binary digit. This loop uses b to save the value of $g^{2^{loopiteration}}$.

sorry I typed these in a hurry!