M328K Homework 13

Joshua Dong

April 30, 2014

0.1 9.3.8

Find a primitive root for 6, 18, 26, and 388.

```python
x = int(raw_input("Find primitive root for: "))

def primes(n):
    primfac = set([])
    d = 2
    while d*d <= n:
        while (n % d) == 0:
            primfac.add(d)
            n /= d
        d += 1
    if n > 1:
        primfac.add(n)
    return primfac

def is_coprime(a, b):
    for p in primes(min(a,b)):
        if max(a,b)%p == 0:
            return False
    return True

def is_complete(g, x):
    complete_mult_group = set(range(1,x))
    for e in list(complete_mult_group):
        if not is_coprime(e, x):
            complete_mult_group.remove(e)
    return g == complete_mult_group

roots = []
for i in xrange(2,x):
    group = set([])
    for j in xrange(1,x):
        result = (i**j)%x
        if not result in group:
            group.add(result)
        else:
            break
    if is_complete(group, x):
        roots.append(i)
print roots
```

We use this program to find all the primitive roots for any integer.
6 has only:

$$5$$

18 has:

$$5, 11$$

26 has:

$$7, 11, 15, 19$$

388 has none.

0.2 9.3.12

Show that there are the same number of primitive roots modulo $2p^t$ as there are modulo p^t, where p is an odd prime and $t \in \mathbb{Z}^+$.

Using Theorem 9.14 from the book, we know that for all primitive roots modulo p^t there exists a corresponding primitive root modulo $2p^t$.
We want to show that for all primitive roots modulo $2p^t$ there exists a corresponding primitive root modulo p^t.
Let r be a primitive root modulo $2p^t$ where p is an odd prime and $t \in \mathbb{Z}^+$.
Then $r^{\varphi(2p^t)} \equiv 1 \pmod{2p^t}$ where $\varphi(2p^t)$ is the lowest exponent such that this is true.
$\varphi(2p^t) = \varphi(2)\varphi(p^t) = \varphi(p^t)$.
$\therefore r^{\varphi(p^t)} \equiv 1 \pmod{2p^t}$.
$\therefore r^{\varphi(p^t)} \equiv 1 \pmod{p^t}$.
We want to show that no smaller power of r is congruent to 1 modulo p^t.
If r is greater than p^t, r corresponds to the primitive root $r - p^t$ modulo p^t.
If r is less than p^t, r is a primitive root modulo p^t.
Therefore, for all primitive roots modulo $2p^t$ there exists a primitive root modulo p^t.
Therefore there exists a one-to-one correspondence from primitive roots of $2p^t$ to primitive roots of p^t.
Therefore there are the same number of primitive roots modulo $2p^t$ as there are modulo p^t, where p is an odd prime and $t \in \mathbb{Z}^+$.