Homework 9

Chris Powell

A. Silverman 17.5.

(a) Try to use the methods in this chapter to compute the square root of 23 modulo 1279. (The number 1279 is prime.) What goes wrong?

Consider the congruence $x^2 \equiv 23 \pmod{1279}$. As 1279 is prime,

$$\varphi(1279) = 1279^1 - 1279^0 = 1279 - 1 = 1278.$$

But by applying the Euclidean algorithm, we find that

$$\gcd(2, \varphi(1279)) = \gcd(2, 1728) = 2 > 1.$$

So by Exercise 17.3.b, either $x^2 \equiv 23 \pmod{1279}$ has no solution or it has at least two solutions.

(b) More generally, if p is an odd prime, explain why the methods in this chapter cannot be used to find square roots modulo p. We will investigate the problem of square roots modulo p in later chapters.

Consider the congruence $x^2 \equiv b \pmod{p}$. Assume p is an odd prime. Then

$$\varphi(p) = p^1 - p^0 = p - 1 \equiv 0 \pmod{2}.$$

So $\gcd(2, \varphi(p)) = 2 > 1$. Thus by Exercise 17.3.b, either$x^2 \equiv b \pmod{p}$ has no solution or it has at least two solutions.

(c) Even more generally, explain why our method for computing k^{th} roots modulo m does not work if $\gcd(k, \varphi(m)) > 1$.

Consider the congruence $x^k \equiv b \pmod{m}$. Suppose $g = \gcd(2, \varphi(m)) > 1$. Let $u, v \in \mathbb{Z}$. Then since $g \mid k, \varphi(m)$, $g \mid ku - \varphi(m)v$. Thus $ku - \varphi(m)v = g \cdot d$ for some $d \in \mathbb{Z}$. But $g > 1$, so $g \nmid ku - \varphi(m)v$.

B. Silverman 17.6. Write a program to solve $x^k \equiv b \pmod{m}$.

```
def gcd(a, b):
    """Return gcd(a,b)"""
    while b:
        a, b = b, a % b
    return a


def xgcd(a, b):
    """Return (g, x, y) such that a*x + b*y = g = gcd(a, b)"""
    if b == 0:
        return a, 1, 0
    x, g, v, w = 1, a, 0, b
    while w != 0:
        x, g, v, w = v, w, x - (g // w) * v, g % w
    x = x % (b // g)
    return g, x, (g - (a * x)) // b


def expmod(a, k, m):
    """compute a^k mod m"""
    b = 1
    while k:
        if k % 2 == 1:
            b = (b * a) % m
        a, k = (a ** 2) % m, k // 2
    return b


def modroot(k, b, m):
    """return x such that x^k cong b mod m if gcd(b,m)=1, gcd(
       k, totient(m)"""
    if gcd(b, m) == 1:
        (g, u, v) = xgcd(k, totient(m))
        print(g, u, v)
        if g == 1:
            return expmod(b, u, m)
```

Note that `modroot` requires $\gcd(b, m) = \gcd(k, \varphi(m)) = 1$.

C. Silverman 18.2. It may appear that RSA decryption does not work if you are unlucky enough to choose a message a that is not relatively prime to m. Of course, if $m = pq$ and p and q are large, this is very unlikely to occur.

(a) Show that in fact RSA decryption does work for all messages a, regardless of whether or not they have a factor in common with m.

If $m = pq$, where p and q are distinct primes, then provided $\gcd(k, \varphi(m)) = 1$, Exercise 17.4.a implies that $x \equiv b^u \pmod{m}$ is always a solution to $x^k \equiv b \pmod{m}$ (even if $\gcd(b, m) > 1$). Thus RSA decryption works for all messages a, regardless of whether or not they have a common factor.

(b) More generally, show that RSA decryption works for all messages a as long as m is a product of distinct primes.

By the Fundantemal Theorem of Arithmetic, we know the RSA modulus m can be factored into a product of distinct primes. Assume k is such that $\gcd(k, \varphi(m)) = 1$. Then this statement follows from the Exercise 17.4, which we proved in the previous homework assignment.

(c) Give an example with $m = 18$ and $a = 3$ where RSA decryption does work. [Remember, k must be chosen relatively prime to $\varphi(m) = 6$.]

Observe that

$$\varphi(m) = \varphi(18) = \varphi(2)\varphi(3^2) = (2-1)(3^2 - 3^1) = 6.$$

Note that $k = 5$ is the least positive integer for which $\gcd(k, 6) = 1$. So

$$a^5 = 3^5 \equiv 9 \pmod{18}.$$

By applying the extended Euclidean algorithm we find that $(u, v) = (5, 4)$ satisfies

$$5u - 6v = 1.$$

D. Silverman 18.4. Here are two longer messages to decode if you like to use computers.

(a) You have been sent the following message:

5272281348,	21089283929,	311723025,
26945939925,	26844144908,	22890519533,
27395704341,	2253724391,	1481682985,
2163791130,	13583590307,	5838404872,
12165330281,	28372578777,	7536755222,

It has been encoded using $p = 187963$, $q = 163841$, $m = pq = 30796045883$, and $k = 48611$. Decode the message.

```
def modrootpq(k, b, m, p, q):
    """given p,q, return x such that x^k cong b mod m=pq
        if gcd(b,m)=1, gcd(k, totient(m))"""
    if gcd(b, m) == 1:
        (g, u, v) = xgcd(k, totient(p)*totient(q))
        if g == 1:
            return expmod(b, u, m)


def rsa_decrypt(k, B, m, p, q):
    "Decrypt RSA ciphertext B given k, m, p, q"
    a = ""
    for b in B:
        a += str(modrootpq(k, b, m, p, q))
    A, a = [chr(int(a)+54) for a in [a[i:i + 2] for i in
        range(0, len(a), 2)]], ""
    for i in A:
        a += i
    return a


B = [5272281348, 21089283929, 3117723025, 26844144908,
    22890519533,
    26945939925, 27395704341, 2253724391, 1481682985,
        2163791130,
    13583590307, 5838404872, 12165330281, 28372578777,
        7536755222]
k = 48611
m = 30796045883
p = 187963
q = 163841

print(rsa_decrypt(k, B, m, p, q))
```

```
MATHEMATICSISTHEQUEENOFSCIENCEANDNUMBERTHEORY
ISTHEQUEENOFMATHEMATICSKFGAUSS
```

(b) You intercept the following message, which you know has been encoded using the modulus

$$m = 956331992007843552652604425031376690367$$

and exponent $k = 12398737$. Break the code and decipher the message.

```
821566670681253393182493050080875560504,
87074173129046399720949786958511391052,
552100909946781566365272088688468880029,
491078995197839451033115784866534122828,
172219665767314444215921020847762293421.
```

E. Silverman 12.1. Start with the list consisting of a single prime $\{5\}$ and use ideas in Euclid's proof that there infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)

Let $S_0 = \{5\}$. We use Euclid's idea to proceed as follows:

$$\begin{aligned}
A_1 &= 5 + 1 = 6 = 2 \cdot 3 & S_1 &= S_0 \cup \{2, 3\} \\
A_2 &= (2 \cdot 3 \cdot 5) + 1 = 31 & S_2 &= S_1 \cup \{31\} \\
A_3 &= (2 \cdot 3 \cdot 5 \cdot 31) + 1 = 931 = 7^2 \cdot 19 & S_3 &= S_2 \cup \{7, 19\} \\
A_4 &= (2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 31) + 1 = 123691
\end{aligned}$$

Since $123691 > 1000$, and thus difficult to factor, the list of primes is

$$\bigcup_{i=0}^{3} S_i = \{2, 3, 5, 7, 19, 31\}.$$

F. Silverman 12.2.

(a) Show that there are infinitely many primes that are congruent to 5 modulo 6. [*Hint*. Use $A = 6p_1p_2 \cdots p_r + 5$).]

Lemma. Let $p > 3$ be prime integer. Then $[p]_6 \in \{ [1]_6, [5]_6 \}$.

Proof. Since $\mathbb{Z}_6 = \{ [0]_6, \ldots, [5]_6 \}$ forms a partition of $\mathbb{Z}$, we know $[p]_6 = [x]_6$ for exactly one $x \in \mathbb{Z}_6$. Suppose $[p]_6 = [0]_6$. Then $p = 6k = 2(3k)$ for some $k \in \mathbb{Z}$. So $p > 3$ is even, contradicting primality of p. The argument is similiar for $[p]_6 \in \{ [2]_6, [3]_6, [4]_6 \}$. Therefore, $[p]_6 \in \{ [1]_6, [5]_6 \}$. □

Proof. Suppose there are only finitely many primes congruent to 5 modulo 6. Let

$$S = \{ 5, p_1 \ldots, p_r \}$$

be those primes. Consider $A = 6 \left(\prod_{i=1}^{r} p_i \right) + 5$. We know A is not prime since $[A]_6 = [5]_6$, but $A \notin S$. So A has prime factorization $A = \prod_{i=1}^{s} q_i$, where each q_i is a distinct. I claim that $[q_i]_6 = [5]_6$ for some i. Suppose $q_i \mid 6$ for some i. Then since $q_i \mid A$,

$$q_i \mid A - 6 \left(\prod_{i=1}^{r} p_i \right) = 5.$$

Thus $q_i = 5$ since the only prime divisor of 5 is 5. But this is a contradiciton since $5 \nmid 6$. Thus $2, 3 \notin S$ and so $[q_i]_6 \in \{ [1]_6, [5]_6 \}$ for all i, by the above lemma. Now it cannot be that $[q_i]_6 = [1]_6$ for all i, as then $[A]_6 = [1]_6$, a contradiction. So there must exist some q_k for which $[q_k]_6 = [5]_6$, as claimed. But clearly $q_k \mid A$, and yet no $x \in S$ divides A by construction. So $q_k \notin S$. Therefore, our original suppositon that there are finitely many primes congruent to 5 modulo 6 is false. The result follows. □

(b) Try to use the same idea (with $A = 5p_1p_2 \cdots p_r + 4$) to show that there are infinitely many primes congruent to 4 modulo 5. What goes wrong? In particular, what happens if you start with $\{ 19 \}$ and try to make a longer list?

In the proof of part (a), we showed that if $A = m\left(\prod_{i=1}^{r} p_i\right) + b$ is not prime, then at least one of its prime factors is congruent to b modulo m, where $(b, m) = (5, 6)$. However, this is not the case for $(b, m) = (4, 5)$. Observe that if we start with $\{19\}$ and compute

$$A = 4(19) + 5 = 99 = 3^2 \cdot 11^1,$$

we see that A is not prime and none of its prime factors are congruent to $4 \pmod 5$: $[11]_5 = [1]_5$. Note that this prime factorization of A is unique (up to rearrangement). So the argument used in part (a) cannot be applied to this case.