Homework 10

Chris Powell

A. Silverman 20.3. A number a is called a *cubic residue modulo* p if it is congruent to a cube modulo p, that is, if there is a number b such that $a \equiv b^3 \pmod{p}$.

(a) Make a list of all the cubic residues modulo 5, modulo 7, modulo 11, and modulo 13.

Observe that

$$\begin{aligned}
\left[0^3\right]_5 &= [0]_5^3 = [0]_5 \\
\left[1^3\right]_5 &= [1]_5^3 = [1]_5 \\
\left[2^3\right]_5 &= [8]_5 = [3]_5 \\
\left[3^3\right]_5 &= [27]_5 = [2]_5 \\
\left[4^3\right]_5 &= [64]_5 = [4]_5
\end{aligned}$$

$$\begin{aligned}
\left[0^3\right]_7 &= [0]_7^3 = [0]_7 \\
\left[1^3\right]_7 &= [1]_7^3 = [1]_7 \\
\left[2^3\right]_7 &= [8]_7 = [1]_7 \\
\left[3^3\right]_7 &= [27]_7 = [6]_7 \\
\left[4^3\right]_7 &= [64]_7 = [1]_7 \\
\left[5^3\right]_7 &= [125]_7 = [6]_7 \\
\left[6^3\right]_7 &= [216]_7 = [6]_7
\end{aligned}$$

$$\begin{aligned}
\left[0^3\right]_{11} &= [0]_{11}^3 = [0]_{11} \\
\left[1^3\right]_{11} &= [1]_{11}^3 = [1]_{11} \\
\left[2^3\right]_{11} &= [8]_{11} = [8]_{11} \\
\left[3^3\right]_{11} &= [27]_{11} = [5]_{11} \\
\left[4^3\right]_{11} &= [64]_{11} = [9]_{11} \\
\left[5^3\right]_{11} &= [125]_{11} = [4]_{11} \\
\left[6^3\right]_{11} &= [216]_{11} = [7]_{11} \\
\left[7^3\right]_{11} &= [343]_{11} = [2]_{11} \\
\left[8^3\right]_{11} &= [512]_{11} = [6]_{11} \\
\left[9^3\right]_{11} &= [729]_{11} = [3]_{11} \\
\left[10^3\right]_{11} &= [1000]_{11} = [10]_{11}
\end{aligned}$$

$$\begin{aligned}
\left[0^3\right]_{13} &= [0]_{13}^3 = [0]_{13} \\
\left[1^3\right]_{13} &= [1]_{13}^3 = [1]_{13} \\
\left[2^3\right]_{13} &= [8]_{13} = [8]_{13} \\
\left[3^3\right]_{13} &= [27]_{13} = [1]_{13} \\
\left[4^3\right]_{13} &= [64]_{13} = [12]_{13} \\
\left[5^3\right]_{13} &= [125]_{13} = [4]_{13} \\
\left[6^3\right]_{13} &= [216]_{13} = [8]_{13} \\
\left[7^3\right]_{13} &= [343]_{13} = [5]_{13} \\
\left[8^3\right]_{13} &= [512]_{13} = [8]_{13} \\
\left[9^3\right]_{13} &= [729]_{13} = [1]_{13} \\
\left[10^3\right]_{13} &= [1000]_{13} = [12]_{13} \\
\left[11^3\right]_{13} &= [1331]_{13} = [5]_{13} \\
\left[12^3\right]_{13} &= [1728]_{13} = [12]_{13}
\end{aligned}$$

So $a \in \{0, 1, 2, 3, 4\}$ if $p = 5$, $a \in \{0, 1, 6\}$ if $p = 7$, $a \in \{0, \ldots, 10\}$ if $p = 11$, and $a \in \{0, 1, 5, 8, 12\}$ if $p = 13$.

(b) Find two numbers a_1 and b_1 such that neither a_1 nor b_1 is a cubic residue modulo 19, but $a_1 b_1$ is a cubic residue modulo 19. Similarly, find two numbers a_2 and b_2 such that none of the three numbers a_2, b_2, or $a_2 b_2$ is a cubic residue modulo 19.

```python
def residue(n, p):
    """Return each a cong b^n mod p for some integer b and
        modulus p; n=2,3"""
    R = []
    for i in range(p):
        R += [(i**n) % p]
    return set(R)
```

Proof. It is clear that the program terminates since it iterates via a `for` loop. Let R_i be the value of the list `R` after the i^{th} iteration. Assume the value of the parameter `n` is 3. At each iteration, R_i is a collection of integers $x_0, \ldots, x_{i-1}$ such that $[x_k]_p = [i_k^n]_p$ for some $i_k \in \mathbb{Z}$ where $i \in \{0, \ldots, p-1\}$. Therefore, by definition, R_i is a list of cubic residues modulo p. The program returns `set(R)`, giving all distinct elements of in the list R_{p-1}. This concludes the proof of correctness. $\square$

By the above algorithm, the set of cubic residues modulo 19 is

$$R = \{0, 1, 7, 8, 11, 12, 18\}.$$

Consider $a_1 = 3$ and $b_1 = 9$. Then

$$[a_1]_{19} \cdot [b_1]_{19} = [3]_{19} \cdot [9]_{19} = [3 \cdot 9]_{19} = [27]_{19} = [8]_{19}\,.$$

Note that $8 \in S$, yet neither 3 nor 9 are in R. Next, consider $a_2 = 4$ and $b_2 = 6$. Then

$$[a_1]_{19} \cdot [b_1]_{19} = [4]_{19} \cdot [6]_{19} = [4 \cdot 6]_{19} = [24]_{19} = [5]_{19}\,.$$

But $4, 5, 6 \notin R$.

(c) If $p \equiv 2 \pmod 3$, make a conjecture as to which a's are cubic residues. Prove that your conjecture is correct.

Conjecture. If $p \equiv 2 \pmod 3$, then every integer not divisible by p is a cubic residue modulo p.

Proof. Let $a \in \mathbb{Z}$ such that $p \nmid a$. Assume $[p]_3 = [2]_3$. Then $3 \mid p-2$. So $p - 2 = 3k$ for some $k \in \mathbb{Z}$. Thus $p = 3k+2$ which implies $p - 1 = 3k + 1$. Since p is prime and $[a]_p \neq [0]_p$, Fermat's Little Theorem implies $\left[a^{3k+1}\right]_p = [1]_p$. It follows that $\left[a^{3k+2}\right]_p = [a]_p$. Thus

$$\begin{aligned}
[a]_p &= [a]_p \cdot [1]_p \\
&= \left[a^{3k+1}\right]_p \cdot \left[a^{3k+2}\right]_p \\
&= \left[a^{3k+1} \cdot a^{3k+2}\right]_p \\
&= \left[a^{6k+3}\right]_p \\
&= \left[a^{3(2k+1)}\right]_p \\
&= \left[\left(a^{(2k+1)}\right)^3\right]_p .
\end{aligned}$$

□

B. Suppose that p is a prime with $p \equiv 1 \pmod 3$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

(a) Show that if a is a cubic residue, then $a^{(p-1)/3} \equiv 1 \pmod p$.

Proof. Suppose $[a]_p = \left[b^3\right]_p$ for some $b \in \mathbb{Z}$. Then

$$\left[a^{(p-1)/3}\right]_p = \left[\left(b^3\right)^{(p-1)/3}\right]_p = \left[b^{p-1}\right]_p .$$

Since $[a]_p \neq [0]_p$, and $\mathbb{Z}_p$ is an integral domain, the zero-product property implies $\left[b^3\right]_p = [b]_p^3 \neq [0]_p$ Therefore, since p is prime, it follows from Fermat's Little Theorem that $\left[b^{p-1}\right]_p = [1]_p$. Hence, $\left[a^{(p-1)/3}\right]_p = [1]_p$. $\square$

C. Write a program that implements the CRT for an arbitrary list of moduli. The input should be a list of ordered pairs $[(a_1, m_1), (a_2, m_2), \ldots, (a_n, m_n)]$ where the m_i are pairwise relatively prime, and the output should be a such that $a \equiv a_i \pmod{m_i}$ for all i. Remember to prove your algorithm works!

```
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 CRT(L):
    """Given (a1,m1),...,(an,mn) with gcd(mi,mj)=1, return x such
        that x = ai (mod mi) for all i"""
    x, M = 0, 1
    for i in range(len(L)):
        M *= L[i][1]
    for i in range(len(L)):
        x += L[i][0] * (M // L[i][1]) * (xgcd(M//L[i][1], L[i][1])
            [1] % L[i][1])
    return x % M
```

Proof. Termination must occur since the program iterates via `for`. I show correctness. The input is a list of ordered pairs $(a_1, m_1), \ldots, (a_n, m_n)$, where the m_i are pairwise relativey prime. Let M be the value of `M` after completion of the first `for` loop. Then clearly, $M = \prod_{k=1}^{n} m_k$. Now consider the program's execution after completion of the first `for` loop. Let x_i be the value of `x` after the i^{th} iteration. Recall that for relatively prime integers a and b, `xgcd(a,b)` returns $(\gcd(a, b), u, v)$, where $[u]_b = [a]_b^{-1}$ and $[v]_b = [b]_a^{-1}$. The program returns

$$[x_n]_M = \left[\sum_{i=1}^{n} \left(a_i \cdot \frac{M}{m_i} \cdot \left[\frac{M}{m_i}\right]_{m_i}^{-1}\right)\right]_M .$$

Therefore, by the Generalized Chinese Remainder Theorem, the program gives the correct output. $\square$

D. Let $f(x)$ be a polynomial, and suppose $m, n \in N$ with $\gcd(m, n) = 1$. Show that $f(x) \equiv 0 \pmod{mn}$ has a solution if and only if $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$ both have solutions.

Proof. Suppose $[f(a)]_m = [0]_m$ and $[f(b)]_n = [0]_n$ for some $a, b \in \mathbb{Z}$. Since $\gcd(m, n) = 1$, the Chinese Remainder Theorem implies there is a unique $c \in \mathbb{Z}_{mn}$ such that $[c]_m = [a]_m$ and $[c]_n = [b]_n$. Thus $[f(c)]_m = [0]_m$ and $[f(c)]_n = [0]_n$. Applying the Chinese Remainder Theorem again, we that $[f(c)]_{mn} = [0]_{mn}$. Conversely, assume $[f(c)]_{mn} = [0]_{mn}$. Then $mn \mid f(x)$. So $f(x) = mnk$ for some $k \in \mathbb{Z}$. By multiplicative associativity and commutativity of $\mathbb{Z}$,

$$f(x) = m(nk) = n(mk).$$

Thus, by multiplicative closure of $\mathbb{Z}$, $m, n \mid f(x)$. Hence, $[f(x)]_m = [0]_m$ and $[f(x)]_n = [0]_n$. $\square$

E. (a) Find all solutions to $x^2 \equiv 1 \pmod{143}$ using the Chinese Remainder Theorem.

The composite modulus 143 has factorization $143 = 11 * 13$, where 11 and 13 are distinct primes. Consider the congruences

$$\left[x^2\right]_{11} = [1]_{11} \quad \text{and} \quad \left[x^2\right]_{13} = [1]_{13}\,.$$

Observe that

$$\begin{aligned}\left[x^2\right]_{11} = [1]_{11} &\Leftrightarrow \left[x^2\right]_{11} - [1]_{11} = [0]_{11}\\ &\Leftrightarrow \left[x^2 - 1\right]_p = [0]_{11}\\ &\Leftrightarrow [(x+1)(x-1)]_{11} = [0]_{11}\,.\end{aligned}$$

As 11 is prime, $\mathbb{Z}_{11}$ is an integral domain. So by the zero-product property, either

$$[x+1]_{11} = [0]_{11} \quad \text{or} \quad [x-1]_{11} = [0]_{11}\,.$$

So either

$$[x]_{11} = -[1]_{11} = [-1]_{11} = [10]_{11} \quad \text{or} \quad [x]_{11} = [1]_{11}\,.$$

Similarly, either

$$[x+1]_{13} = [0]_{13} \quad \text{or} \quad [x-1]_{11} = [0]_{13}\,.$$

So either

$$[x]_{13} = -[1]_{13} = [-1]_{13} = [12]_{13} \quad \text{or} \quad [x]_{13} = [1]_{13}\,.$$

By the Chinese Remainder Theorem, there is a unique $x \in \mathbb{Z}_{143}$ such that

$$\begin{cases}[x]_{11} = [1]_{11}\\ [x]_{13} = [1]_{13}\,,\end{cases} \quad \begin{cases}[x]_{11} = [10]_{11}\\ [x]_{13} = [1]_{13}\,,\end{cases} \quad \begin{cases}[x]_{11} = [1]_{11}\\ [x]_{13} = [12]_{13}\,,\end{cases} \quad \begin{cases}[x]_{11} = [10]_{11}\\ [x]_{13} = [12]_{13}\,.\end{cases}$$

Using the `CRT` program from Exercise C, I get solutions

$$[1]_{143}\,, [131]_{143}\,, [12]_{143}\,, [142]_{143}\,,$$

respectively.

(b) Let p, q be distinct primes. How may solutions does $x^2 \equiv 1 \pmod{pq}$ have?

Proof. Assume p and q are odd primes. Observe that

$$\begin{aligned}\left[x^2\right]_p = [1]_p &\Leftrightarrow \left[x^2\right]_p - [1]_p = [0]_p \\ &\Leftrightarrow \left[x^2 - 1\right]_p = [0]_p \\ &\Leftrightarrow [(x+1)(x-1)]_p = [0]_p .\end{aligned}$$

Since $\mathbb{Z}_p$ is an integral domain, it follows from the zero-product property that either $[x+1]_p = [0]_p$ or $[x-1]_p = [0]_p$. But we cannot have both $[x+1]_p = [0]_p$ and $[x-1]_p = [0]_p$, as then $p \mid x+1, x-1$ which implies

$$p \mid (x+1) - (x-1) = 2,$$

a contradiction since $p > 2$. Now if $[x+1]_p = [0]_p$, then $[x]_p = [-1]_p$. On the other hand, $[x-1]_p = [0]_p$ implies that $[x]_p = [1]_p$. Thus the congruence $\left[x^2\right]_p = [1]_p$ has exactly 2 solutions, namely, $[\pm 1]_p$; likewise $\left[x^2\right]_q = [1]_q$ has solutions $[\pm 1]_q$. By the Chinese Remainder Theorem, there is a unique $x \in \mathbb{Z}_{pq}$ such that $[x]_p = [a]_p$ and $[x]_q = [b]_p$ for each $(a, b) \in \{ [\pm 1]_p \} \times \{ [\pm 1]_q \}$. Hence the congruence $\left[x^2\right]_p = [1]_p$ has exactly $2^2 = 4$ solutions. If p or q is 2, then there are exactly 2 solutions since $[1]_2 = [-1]_2$. □

(c) Let $p_1, p_2, \ldots, p_r$ be distinct primes. How many solutions does $x^2 \equiv 1 \pmod{p_1 p_2 \cdots pr}$ have?

Proof. Assume that each prime p_i is odd. Let $m = \prod_{i=0}^{r} p_i$. Then by the Generalized Chinese Remainder Theorem, there is a unique $x \in \mathbb{Z}_m$ such that $[x]_{p_i} = [a_i]_{p_i}$ for all $i \in \{1, \ldots, r\}$. But by the argument given in part (b), each congruence $\left[x^2\right]_{p_i} = [1]_{p_i}$ has the solutions set $\{ [\pm 1]_{p_i} \}$. In other words, there is exactly one $x \in \mathbb{Z}_m$ satisfying $[x]_{p_i} = [a_i]_{p_i}$ for each $(a_1, \ldots, a_r) \in \{ [\pm 1]_{p_1} \} \times \cdots \times \{ [\pm 1]_{p_r} \}$. Thus $\left[x^2\right]_m = [1]_m$ has exactly 2^r solutions. If $p_i = 2$ some for some i, then there are exactly 2^{r-1} solutions since $[1]_2 = [-1]_2$ □