MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 3 (16pts)

1.6 3; 3pts *Let $a \in \mathbb{Z}^+$. Show that the last digit of a and the last digit of a^5 in base 10 are the same.*

We need to show that $a^5 \equiv a$ mod 10. Since there are only 10 possibilities for $a \mod 10$,

$$a \equiv -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 \mod 10,$$

we can simply check this statement on each of them. Since $(-a)^5 = -a^5$, it is in fact sufficient to check this on the 6 nonnegative choices. On them, we get

$$0^5 = 0, \quad 1^5 = 1, \quad 2^5 = 32 \equiv 2 \mod 10, \quad 3^5 = 243 \equiv 3 \mod 10,$$
$$4^5 = 1024 \equiv 4 \mod 10, \quad 5^5 = 3125 \equiv 5 \mod 10,$$

as needed.

Alternatively, we can use Euler's Theorem with some care. Since $(ab)^5 = a^5 b^5$, it is sufficient to check that $a^5 \equiv a$ mod 10 only for $a = 0, 1$ and the primes $p = 2, 3, 5, 7$ that are smaller that 10. The first two cases are trivial. By Theorems 1.6.6 and 1.6.5,

$$|G_{10}| = |G_{2\cdot 5}| = |G_2| \cdot |G_5| = (2^1 - 2^{1-0})(5^1 - 5^{1-0}) = 4.$$

Since 3 and 7 are relatively prime to 10, $3^4 \equiv 1$ and $7^4 \equiv 1$ mod 10; this implies the desired congruence for $a = 3, 7$. Euler's Theorem does not apply in the two remaining cases, $a = 2, 5$, because they are not relatively prime to 10. In these cases, the congruence is verified as in the previous paragraph.

Another alternative is to use the Chinese Remainder Theorem. Since $10 = 2\cdot 5$ and $\gcd(2, 5) = 1$,

$$a^5 \equiv a \mod 10 \qquad \Longleftrightarrow \qquad \begin{cases} a^5 \equiv a \mod 2 \\ a^5 \equiv a \mod 5 \end{cases}$$

If a is even (resp. odd), then so is a^5; thus, $a^5 \equiv a$ mod 2. Since 5 is prime, $a^5 \equiv a$ mod 5 by Fermat's Little Theorem.

1.6 7; 4pts *Let $n \in \mathbb{Z}$. Show that $n^{13} - n$ is divisible by 2,3,5,7, and 13.*

We need to show that $n^{13} = n$ mod $p = 2, 3, 5, 7, 13$. Since $(ab)^{13} = a^{13} b^{13}$, it is sufficient to check that $n^{13} \equiv n$ mod p only for $n = 0, 1$ and the primes n smaller than p. The first two cases are trivial. Since all primes n smaller than p are relatively prime to p, Euler's Theorem applies. By Theorem 1.6.6,

$$|G_2| = 1, \quad |G_3| = 2, \quad |G_5| = 4, \quad |G_7| = 6, \quad |G_{13}| = 12.$$

Since all these cardinalities divide 12, $n^{12} \equiv 1$ mod each $p = 2, 3, 5, 7, 13$ for every n relatively prime to p. This establishes the desired congruence.

1.6 8; 5pts *Let $n\in\mathbb{Z}^+$ with $n\geq 2$ and p be a prime such that $p|n$, but $p^2\nmid n$. Show that*

$$p^{|G_n|+1}\equiv p \mod n.$$

Can you generalize this statement?

Suppose $m\in\mathbb{Z}$ and

$$r=\max\big\{k\in\mathbb{Z}^{\geq 0}\colon \exists\,\text{prime } p \text{ s.t. } p|m,\ p^k|n\big\}\in\mathbb{Z}^{\geq 0}.$$

We show that

$$m^{|G_n|+r}\equiv m^r \mod n. \tag{1}$$

Let P_m be the set of all primes that divide m. For each $p\in P_m$, let

$$r_p=\max\big\{k\in\mathbb{Z}^{\geq 0}\colon p^k|n\big\}\in\mathbb{Z}^{\geq 0}.$$

Let $d=\prod_{p\in P_m}p^{r_p}$. Thus, d divides m^r and n, and d and m are relatively prime to n/d. If $n/d=1$, then $n=d$ divides both sides of (1) and the equality holds. If $n/d>1$, Theorem 6.1.6 and Euler's Theorem give

$$m^{|G_n|}=m^{|G_{n/d}|\cdot|G_d|}=\big(m^{|G_{n/d}|}\big)^{|G_d|}\equiv 1^{|G_d|}\equiv 1 \mod n/d.$$

This means that n/d divides $m^{|G_n|}-1$ and thus n divides

$$d\big(m^{|G_n|}-1\big)\big(m^r/d\big)=m^{|G_n|+r}-m^r\,.$$

This establishes (1).

1.6 13; 4pts *A public code has base 143 and exponent 103. It uses the following letter-to-number equivalents:*

$$J=1,\quad N=2,\quad R=3,\quad H=4,\quad D=5,\quad A=6,\quad S=7,\quad Y=8,\quad T=9,\quad O=0.$$

Decode the received two-block message 10/03.

By Theorems 1.6.6 and 1.6.5,

$$\big|G_{143}\big|=\big|G_{11\cdot 13}\big|=\big|G_{11}\big|\cdot\big|G_{13}\big|=(11-1)(13-1)=120.$$

Thus, we need to find x so that $103x\equiv 1$ mod 120. Euclid's algorithm with $(103,120)$ gives

$$\begin{aligned}
&(1)\colon\ \mathbf{120}=1\cdot\mathbf{103}+\mathbf{17} &&\gcd(\mathbf{103},\mathbf{120})=\mathbf{1}\overset{(2)}{=\!=}\mathbf{103}-6\cdot\mathbf{17}\\
&(2)\colon\ \mathbf{103}=6\cdot\mathbf{17}+\mathbf{1} &&\overset{(1)}{=\!=}\mathbf{103}-6\cdot(\mathbf{120}-1\cdot\mathbf{103})=7\cdot\mathbf{103}-6\cdot\mathbf{120}.\\
&(3)\colon\ \ \mathbf{17}=17\cdot\mathbf{1}+0
\end{aligned}$$

Thus, $7\cdot 103-6\cdot 120=1$ and we can use $x=7$ as the decoding exponent. Since

$$10^7=1000^2\cdot 10\equiv(-1)^2\cdot 10\equiv 10 \mod 143 \quad\text{and}\quad 3^7=243\cdot 9\equiv 100\cdot 9\equiv 900\equiv 42 \mod 143,$$

the decoded two-block message is 10/42. This corresponds to $\boxed{\text{JOHN}}$