Problem 3 page 82: $8 \equiv (-1) \pmod 3$.

Hence $8^{24} \equiv 1 \pmod 3$. Thus

$3 \mid 8^{24} - 1$ and there exists an integer q, such that

$$8^{24} = 3q + \underbrace{1}_{\text{Remainder.}}$$

Exercise set 3

Problem 6 page 82

Is $6^{17} + 17^6$ divisible by 3 or 7?

Modulo 3:

$3 \mid 6 \Rightarrow 3 \mid 6^{17}$, so $6^{17} \equiv 0 \pmod 3$.

$17 \equiv -1 \pmod 3$.

Prop 3.12

So $17^6 \equiv (-1)^6 \equiv 1 \pmod 3$.

Hence $6^{17} + 17^6 \equiv 0 + 1 \equiv 1 \pmod 3$

Prop 3.12

Hence $3 \nmid (6^{17} + 17^6)$.

Modulo 7:

$6 \equiv -1 \pmod 7$. Hence $6^{17} \equiv (-1)^{17} \equiv -1 \pmod 7$.

$17 \equiv 3 \pmod 7$. Hence,

$17^3 \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$. So,

$17^6 \equiv (-1)^2 \equiv 1 \pmod 7$

Thus $6^{17} + 17^6 \equiv (-1) + 1 \equiv 0 \mod 7$.

We conclude that 7 divides $6^{17} + 17^6$.

Problem 10 page 83:

There does not exist a positive integer k, such that $2^k \equiv 1 \pmod{14}$.

Proof: By contradiction. Assume such k exists.
$2 \mid 2^k$, since k is a positive.
Hence $14 \mid (7 \cdot 2^k)$ and $7 \cdot 2^k \equiv 0 \pmod{14}$.
But, the assumption $2^k \equiv 1 \pmod{14}$
implies that $7 \cdot 2^k \equiv 7 \pmod{14}$.
Hence $1 \equiv 7 \pmod{14}$. A contradiction,
since $14 \nmid (7-1)$.

Q.E.D

Remark: Another proof (shorter) uses Prop 3.53, which has not been covered yet in class.

Problem 30 page 82:

Multiplication in $\mathbb{Z}_8$

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Multiplicative inverses exist only for [1], [3], [5], [7] and the inverse of each in $\mathbb{Z}_8$ is itself.