Homework 8
MME 529

1. What is the prime factorization of 1,005,010,010,005,001?

Answer: $1,005,010,010,005,001$

$= 143,572,858,572,143 \cdot 7$
$= 20,510,408,367,449 \cdot 7^2$
$= 2,930,058,338,207 \cdot 7^3$
$= 418,579,762,601 \cdot 7^4$
$= 59,797,108,943 \cdot 7^5$
$= 5,436,100,813 \cdot 11 \cdot 7^5$
$= 371,293 \cdot 11^5 \cdot 7^5$
$= 28,561 \cdot 13 \cdot 11^5 \cdot 7^5$
$= 13^5 \cdot 11^5 \cdot 7^5$.

Alternatively, if one knows that $1,001^5 = n$
$= 1,005,010,010,005,001$, the use $1,001 = 13 \cdot 11 \cdot 7$
to get $n = (13 \cdot 11 \cdot 7)^5 = 13^5 \cdot 11^5 \cdot 7^5$.

2. Simplify $(3333^{4444} + 4444^{3333}) \bmod 7$

Answer:

$$
\begin{array}{r}
476 \\
7\overline{)3333} \\
-2800 \\
\hline
533 \\
-490 \\
\hline
43 \\
-42 \\
\hline
1
\end{array}
$$

$3333 \equiv 1 \bmod 7$

$3333^{4444} \equiv 1 \bmod 7$

$$
\begin{array}{r}
634 \\
7\overline{)4444} \\
-4200 \\
\hline
244 \\
-210 \\
\hline
34 \\
-28 \\
\hline
6
\end{array}
$$

$4444 \equiv 6 \bmod 7$

$4444^2 \equiv 6^2 \bmod 7 \equiv 1 \bmod 7$

$4444^{3333} = 4444^{3332}\,4444$

$= (4444^2)^{1666}\,4444$

$\equiv 1^{1666} \cdot 6 \bmod 7$

$\equiv 6 \bmod 7$

$$(3333^{4444} + 4444^{3333}) \equiv (6+1) \bmod 7 \equiv 0 \bmod 7.$$

3. Find generators for the subgroups G_1 and G_2 of $\mathbb{Z}_{19}$ where multiplication is the binary operation and

$$G_1 = \{1, 4, 5, 6, 7, 9, 11, 16, 17\},$$
$$G_2 = \{1, 7, 8, 11, 12, 18\}.$$

Answer: Use code similar to

```
For g in G1 (or G2):
    For i = 1:|G1| (or |G2|):
        print g^i mod 19
    end
end
```

And see for which $g \in G_1$ ($g \in G_2$), all elements of the subgroup are listed.

G_1 is generated by 4, 5, 6, 16, 17. G_2 is generated by 8 and 12.

4. Consider the group under multiplication

$$G = \{\pm 1, \pm i, (\pm 1 \pm i)/\sqrt{2}\}.$$

a) Find a nontrivial subgroup of G.
b) Identify a generator of G.

Answer:

a) $G_1 = \{\pm 1, \pm i\}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From this table we see that G_1 satisfies the group axioms.

b) $g = \frac{1+i}{\sqrt{2}}$

$g^2 = i$

$g^3 = \frac{-1+i}{\sqrt{2}}$

$g^4 = -1$

$g^5 = \frac{-1-i}{\sqrt{2}}$

$g^6 = -i$

$g^7 = \frac{1-i}{\sqrt{2}}$

$g^8 = 1$

$\therefore g = (1+i)/\sqrt{2}$ is a generator of G.

5. Find the group G generated by $A = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$ under matrix multiplication.

Answer:

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad A^5 = A^4A = -A = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad A^6 = A^4A^2 = -A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$A^3 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix} \qquad A^7 = A^4A^3 = -A^3 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad A^8 = A^4A^4 = I_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

6. Find the group G generated by $g = e^{i\pi/6}$ under ordinary multiplication.

Answer:

$g = e^{i\pi/6}$

$g^2 = e^{i\pi/3}$

$g^3 = e^{i\pi/2}$

$g^4 = 2^{i\pi/3}$

$g^5 = e^{5i\pi/6}$

$g^6 = e^{i\pi}$

$g^7 = e^{7\pi i/6}$

$g^8 = e^{4\pi i/3}$

$g^9 = e^{3\pi i/2}$

$g^{10} = e^{5\pi i/3}$

$g^{11} = e^{11\pi i/6}$

$g^{12} = e^{2\pi i} = 1$

The group G generated by g are the 12^{th} roots of unity:

$$1 = e^{2\pi k i}$$

$$\sqrt[12]{1} = e^{i\pi k/6} = g^k, \quad k \in \mathbb{Z}.$$

7. What size subgroups would you expect $\mathbb{Z}_{41}$ to have?

Answer: By Lagrange's Theorem, for any subgroup H of the group G, $|H|$ must be a divisor of $|G|$.

Since 41 is prime, this means that for any subgroup H of $\mathbb{Z}_{41}$, $|H| = 1$ or $|H| = 41$.

In particular, we have the subgroups $H_1 = \mathbb{Z}_{41}$ and $H_2 = \{1\}$. For any $g \in \mathbb{Z}_{41}$, $g \neq 1$, the primality of 41 implies that g is a generator of $\mathbb{Z}_{41}$. This means that the only subgroups of $\mathbb{Z}_{41}$ are the trivial subgroups H_1 and H_2.

8. Use Fermat's Factorization method for 5293.

Answer: $n = 5293$

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Find $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$ s.t. $n = x^2 - y^2$
and then solve for a and b.
We have $72^2 < n < 73^2$. Keep trying
$x = 73, 74, 75, \ldots$ until we find $n = x^2 - y^2$.

$$5293 = 73^2 - 36 = 73^2 - 6^2 = x^2 - y^2.$$

So we found y on the first attempt.

$$73 = x = \frac{a+b}{2}, \quad 6 = y = \frac{a-b}{2}$$

$$\rightarrow a = x + y = 73 + 6 = 79$$
$$b = x - y = 73 - 6 = 67$$
$$5293 = n = ab = 79 \cdot 67.$$