Below is a collection of practice problems for midterm 2, many of which are borrowed from previous exams in similar courses. At students' request, I've provided a large collection of problems beyond a single practice exam. If you want to try a "model exam," you can use the first six problems for this purpose.

1. When the students in a classroom divide into groups of nine, there are four students left over. When the students break into groups of eleven, there is one student left over. Assuming that there are fewer than 100 students in the room, how many students must there be?

$n \equiv 4 \bmod 9$

$n \equiv 1 \bmod 11$ $\quad 0 \leq n \leq 99$

$n = 4 + 9k$ where

$4 + 9k \equiv 1 \bmod 11$

$\Leftrightarrow 9k \equiv -3 \bmod 11.$

Need an inverse of 9 modulo 11:

$[2] = (11) - (9)$

$[1] = (9) - 4[2] = (9) - 4(11) + 4(9)$

$= 5(9) - 4(11)$

$\Rightarrow 5 \cdot 9 \equiv 1 \bmod 11.$

Thus

$9k \equiv -3 \bmod 11$

$\Leftrightarrow \underbrace{5 \cdot 9}_{\equiv 1} k \equiv -5 \cdot 3 \bmod 11$

$\Leftrightarrow k \equiv -15 \equiv 7 \bmod 11.$

So

$n = 4 + 9 \cdot (7 + 11 \cdot h) = 4 + 63 + 99h$

i.e. $n \equiv 67 \bmod 99.$

There are $\boxed{\text{67 students,}}$ since $n < 100$.

2. What is the remainder when 10^{100} is divided by 19?

$\gcd(10,19)=1$ & 19 is prime so by Fermat's little theorem.

$$10^{100} = 10^{90}\cdot 10^{10} = (10^{18})^5 \cdot 10^{10}$$
$$\equiv 10^{10} \bmod 19$$

Method 1

$10^1 \equiv 10$

$10^2 \equiv 100 \equiv 5$

$10^4 \equiv 5^2 \equiv 25 \equiv 6$

$10^8 \equiv 6^2 \equiv 36 \equiv -2$

$\Rightarrow 10^{10} \equiv 10^8 \cdot 10^2$

$\equiv -2\cdot 5 \equiv -10$

$\equiv 9 \bmod 19$

Method 2

Compute 10 to these exponents (in reverse order):

10, 5 4 2, 1

$10^1 \equiv 10$

$10^2 \equiv 100 \equiv 5$

$10^4 \equiv 25 \equiv 6$

$10^5 \equiv 6\cdot 10 \equiv 60 \equiv 3$

$10^{10} \equiv 3^2 \equiv 9 \bmod 19$

Method 3

Just mult. by 10 ten times:

$10^1 \equiv 10$

$10^2 \equiv 100 \equiv 5$

$10^3 \equiv 50 \equiv 12$

$10^4 \equiv 120 \equiv 6$

$10^5 \equiv 60 \equiv 3$

$10^6 \equiv 30 \equiv 11$

$10^7 \equiv 110 \equiv 15$

$10^8 \equiv 150 \equiv 17$

$10^9 \equiv 170 \equiv 18$

$10^{10} \equiv 180 \equiv 9.$

Using any method, $10^{100} \equiv 10^{10} \equiv 9 \bmod 19$.

So the remainder is $\boxed{9}$.

3. (a) How many numbers between 1 and 1500 inclusive are relatively prime to 1500 (that is, share no common factors besides 1 with 1500)?

$$\varphi(1500) = \varphi(3\cdot 5\cdot 2^2\cdot 5^2) = \varphi(2^2\cdot 3\ 5^3)$$
$$= (4-2)(3-1)(125-25)$$
$$= \boxed{400}$$

(b) Find the sum of all positive divisors of 1500.

$$\sigma(1500) = \sigma(2^3)\sigma(3)\sigma(5^3) \quad (\sigma \text{ is multiplicative})$$
$$= (1+2+4+8)(1+3)(1+5+25+125)$$
$$= \boxed{31\cdot 4\cdot 165} \quad (\text{fine to leave arithmetic unsimplified})$$

(c) Find the remainder when 1493^{2002} is divided by 1500.

Eulers thm:

$2002 \equiv 2 \bmod \varphi(1500)$ and $\gcd(1493, 1500)$
$= \gcd(1500, 7) = 1$

$\Rightarrow 1493^{2002} \equiv 1493^2 \bmod 1500$

Now observe $1493 \equiv (-7) \bmod 1500$

so $1493^2 \equiv (-7)^2 \equiv 49 \bmod 1500.$

The remainder is $\boxed{49}$.

4. Prove that there are infinitely many prime numbers p such that $p \equiv 3 \pmod 4$.

Suppose $3, p_1, p_2, \cdots, p_{r-1}$ are r such primes.

Let $A = 4p_1p_2\cdots p_{r-1} + 3$.

Then $A \equiv 3 \bmod 4$, $3 \nmid A$ (since $3 \nmid 4p_1\cdots p_{r-1}$)

and $p_i \nmid A$ for $i = 1, 2, \cdots, r-1$

since $p_i \nmid 3$.

Now, at least one prime factor q of A is $\equiv 3 \bmod 4$

since otherwise all are $\equiv 1 \bmod A$ (none is 2 or 4 mod 4

since A is odd) & $A \equiv 1 \cdot 1 \cdots 1 \bmod 4$.

So q is a prime $\equiv 3 \bmod 4$ other than $3, p_1, \cdots, p_{r-1}$.

Therefore we can always find one more such prime

ie. there are infinitely many.

Since this is a fact that was proved in class, you should not simply cite the theorem from class, but rather give a proof. This is true for any other exam problems that ask you to prove a fact that was proved in class.

5. Let $n \geq 2$ be an integer such that $p = \frac{1}{2}(3^n - 1)$ is prime. Prove that n is also prime.

$\neg$ Suppose that n is not prime. Then $n = ab$ for some $a, b \geq 2$.

Now,

$$3^n - 1 = 3^{ab} - 1 = (3^a)^b - 1$$

is divisible by $3^a - 1$ by the factorization

$$(3^a - 1)((3^a)^{b-1} + (3^a)^{b-2} + \dots + 3^a + 1).$$

Since $3^a - 1$ is even, $\frac{1}{2}(3^a - 1)$ is an (integer) divisor of $\frac{1}{2}(3^n - 1)$.

Since $1 < a < ab$, we have

$$3^1 - 1 < 3^a - 1 < 3^{ab} - 1$$

i.e. $$2 < 3^a - 1 < 3^n - 1$$

$$\Rightarrow \quad 1 < \frac{1}{2}(3^a - 1) < \frac{1}{2}(3^n - 1).$$

So this is a divisor of $\frac{1}{2}(3^n - 1)$ that isn't 1 or itself.

So $\frac{1}{2}(3^n - 1)$ isn't prime. $\lightning$.

6. Suppose that p is a prime number, and a, b are integers such that $e_p(a) = 2$ and $e_p(b) = 3$. Prove that $e_p(ab) = 6$.

By def'n of order, we have

$$a \not\equiv 1, \quad a^2 \equiv 1 \bmod p$$

& $b \not\equiv 1, \; b^2 \not\equiv 1, \; b^3 \equiv 1 \bmod p.$

From this, it follows that

$$(ab)^6 \equiv a^6 b^6 \equiv 1^3 \cdot 1^2 \equiv 1 \bmod p$$

so $e_p(ab) \mid 6$ (since $a^n \equiv 1 \iff e_p(a) \mid n$).

This means order is one of 1, 2, 3, or 6.

Now,

$$(ab)^2 \equiv a^2 b^2 \equiv b^2 \not\equiv 1 \bmod p$$

& $(ab)^3 \equiv a^3 b^3 = a \cdot a^2 \cdot b^3$
$\equiv a \cdot 1 \cdot 1 \equiv a \not\equiv 1 \bmod p,$

so the order cannot be 2 or 3.

It also can't be 1, otherwise $ab \equiv 1 \bmod p$, which would imply $(ab)^2 \equiv 1$, too.

So the only possibility is that $e_p(ab) = 6$.

You can treat the first six problems as a "model exam." The remaining problems below are for additional practice.

7. Suppose that Bob's RSA public key is $(33, 13)$. Alice sends Bob the cipher text $c = 8$. What was Alice's plain text?
(Recall that if s is Alice's plain text, then she computes the cipher text c by computing the remainder when s^{13} is divided by 33.)

$\varphi(33) = \varphi(3\ 11) = (3-1)\cdot(11-1) = 20.$

Deciphering exponent: inverse of 13 mod 20.

(20)
(13)
$[7] = (20) - (13)$
$[6] = (13) - [7] = 2\cdot(13) - (20)$
$[1] = [7] - [6] = 2\cdot(20) - 3\cdot(13).$

So the inverse is -3 or $\underline{17 \bmod 20}$.

Therefore

$s \equiv c^{17} \bmod 33$
$\equiv 8^{17}$

Succ. squaring:
$8^1 \equiv 8$
$8^2 \equiv 64 \equiv -2$
$8^4 \equiv (-2)^2 \equiv 4$
$8^8 \equiv 16$
$8^{16} \equiv 256 \equiv 58 \equiv -8$
$8^{17} \equiv 8^{16}\cdot 8 \equiv (-8)8 \equiv -64 \equiv \underline{2 \bmod 33}$

So the secret is $\boxed{2}$.

<u>Alt. solution</u> (w/ CRT).

Solve separately:
$s^{13} \equiv 8 \bmod 3$
$\iff s \equiv 8 \bmod 3$ (Fermat)
$\iff s \equiv 2 \bmod 3$

and $s^{13} \equiv 8 \bmod 11$
$\iff s^3 \equiv 8 \bmod 11$ (Fermat)
$\iff s \equiv 8^7 \bmod 11$
(since $7\cdot 3 \equiv 1 \bmod \varphi(11)$)

succ. sq. mod 11:
$8^1 \equiv 8$
$8^2 \equiv 64 \equiv 9$
$8^3 \equiv 72 \equiv 6$
$8^6 \equiv 36 \equiv 3$
$8^7 \equiv 3\cdot 8 \equiv 2$
so $s \equiv 2 \bmod 11$

now, since
$s \equiv 2 \bmod 3$
& $s \equiv 2 \bmod 11$
it follows by CRT that
$s \equiv 2 \bmod 33.$

8. Suppose that a, e, f, and m are positive integers such that the following two congruences hold.

$$\begin{aligned} a^e &\equiv 1 \pmod{m} \\ a^f &\equiv 1 \pmod{m} \end{aligned}$$

Prove that

$$a^{\gcd(e,f)} \equiv 1 \pmod{m}.$$

By the Euclidean algorithm there are integers u & v s.t.

$$e u - f \cdot v = \gcd(e, f).$$

We can assume that u, v are positive (otherwise swap to e and f).

Therefore:

$$a^{e \cdot u} \equiv a^{f \cdot v + \gcd(e,f)} \bmod m$$

$$\Rightarrow \quad (a^e)^u \equiv (a^f)^v \cdot a^{\gcd(e,f)} \bmod m$$

$$\Rightarrow \quad 1^u \equiv 1^v \cdot a^{\gcd(e,f)} \bmod m$$

$$\Rightarrow \quad \underline{1 \equiv a^{\gcd(e,f)} \bmod m}.$$

as desired.

9. Let $d(n)$ denote the number of divisors of n, including 1 and n. For example:

$$\begin{aligned} d(10) &= 4 \text{ (the divisors are } 1, 2, 5, 10) \\ d(17) &= 2 \text{ (the divisors are } 1, 17) \\ d(24) &= 8 \text{ (the divisors are } 1, 2, 3, 4, 6, 8, 12, 24) \end{aligned}$$

You may assume the following fact: if $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$ (I encourage you to try to prove it, but you don't need to do it now).

(a) Find a formula for $d(p^k)$, where p is prime and $k \geq 1$.

The divisors are $1, p, p^2, \cdots, p^k$, there are k of them.

$$\boxed{d(p^k) = k+1}$$

(b) Compute $d(91000)$.

$$91000 = 91 \cdot 10^3 = 7 \cdot 13 \cdot 2^3 \cdot 5^3$$

so $d(91000) = d(7)d(13)\,d(2^3)\,d(5^3)$

$= \cancel{8}\,2 \cdot 2\; 4 \cdot 4$

$= \boxed{64}$

(c) Give a simple criterion to tell whether $d(n)$ is even or odd.

If $n = p_1^{e_1} p_1^{e_2} \cdot p_\ell^{e_\ell}$ ($p_1, \cdots, p_\ell$ distinct primes)

then $d(n) = (e_1+1)(e_2+1)\cdots(e_\ell+1)$.

Hence $d(n)$ is odd $\iff$ every exponent e_i is even

$\iff$ n is a perfect square.

$\boxed{\text{Squares have an odd number of divisors, non-squares have an even number of divisors.}}$

Alt solution: any divisor d has a 'partner' n/d The only divisor that is its own partner is $\sqrt{n}$ (if it's an integer).
So if n isn't a square $d(n)$ is even (divisors are paired up in couples)
but if n is a square then $\sqrt{n}$ is left over after the pairing-off.

10. **Short answer questions.** You do not need to show any work. **Several questions have multiple possible answers; you only need to give one.**

(a) Compute the greatest common divisor of 77 and 91.

$91-77=14$
$77-5\cdot 14=7$
$14-2\cdot 7=0$

Answer: 7

(b) Find a perfect number (that is, a positive number which is equal to twice the sum of all of its divisors, including 1 and itself).

Answer: 6 (also 28, 496, etc)

(c) Find the smallest *positive* number of the form $15x+39y$, where x and y are integers (positive or negative).

$\gcd(15,39)$
$=\gcd(15,9)$
$=\gcd(6,9)$
$=\gcd(6,3)=3$

Answer: 3

(d) Find a positive integer n such that $10^n \equiv 1 \pmod{113}$. (The number 113 is prime)

Answer: 112 (F.l.T.)

(e) Evaluate $\phi(130)$.

$130=2\cdot 5\cdot 13$
$\varphi(130)=1\cdot 4\cdot 12$

Answer: 48

(f) Find a primitive root of 7.

powers of 2: 2 4 1 ..
of 3: 3 2 6 4 5 1 ...
of 4: 4 2 1 ..
of 5: 5 4 6 2 3 1 ...
of 6: 6 1 ...

Answer: 3 or 5 (only one needed)

11. Solve the congruence

$$x^{23} \equiv 5 \pmod{29}.$$

Your answer should be in the form $x \equiv a \pmod{m}$, where a is between 0 and $m-1$ inclusive. (You may want to use the multiplication table on the last page.)

Hint. The answer will be congruent to 5^f for a well-chosen value of f.

If $23f \equiv 1 \bmod \varphi(29)$, then $x^{23f} \equiv x^1 \bmod 29$, so $5^f \equiv x$.
Since $\varphi(29) = 28$, we want an inverse of 23 mod 28.
Use the extended euclidean algorithm:

$$\begin{aligned}
&(28)\\
&(23)\\
[5] &= (28) - (23)\\
[3] &= (23) - 4[5]\\
&= 5(23) - 4(28)\\
[1] &= 2\cdot[3] - [5]\\
&= 11(23) - 9(28)
\end{aligned}$$

So $11 \cdot 23 \equiv 1 \bmod 28$ so we know that $x \equiv 5^{11} \bmod 29$.
Use successive squaring. (w/ the mod 29 mult. table).

$$\begin{aligned}
5^1 &\equiv 5\\
5^2 &\equiv 5\cdot 5 = 25\\
5^4 &\equiv 25\cdot 25 \equiv 16\\
5^5 &\equiv 16\cdot 5 \equiv 22\\
5^{10} &\equiv 22\cdot 22 \equiv 20\\
5^{11} &\equiv 5\cdot 20 \equiv 13
\end{aligned}$$

so $\boxed{x \equiv 13 \bmod 29}$

12. Consider the rather large number $N = 2^{53^{69}}$ (Note that this is 2 raised to the power 53^{69}, not 2^{53} raised to the power 69.)

    (a) Find the remainder when N is divided by 4.

$2^2 \mid N$ since $53^{69} \geq 2$ so $\boxed{N \equiv 0 \bmod 4}$.

    (b) Find the remainder when N is divided by 25.

$\varphi(25) = 20$, so we can first reduce 53^{69} mod 20 ($\gcd(2,25)=1$).
similarly $\varphi(20) = 16$. so we can first reduce 69 mod 16
$69 \equiv 5 \bmod 16$, so $53^{69} \equiv 53^5 \bmod 20$
$53 \equiv 13 \bmod 20$, so also $53^5 \equiv 3^5 \bmod 20$
Now, mod 20.
$13^1 \equiv -7$
$13^2 \equiv 49 \equiv 9$
$13^4 \equiv 9^2 \equiv 81 \equiv 1$
$13^5 \equiv 13 \bmod 20$.
Thus $\cancel{53} \cdot 53^{69} \equiv 13 \bmod 20$ hence $N \equiv 2^{13} \bmod 25$.

By successive squaring
$2^1 \equiv 2 \bmod 25$
$2^2 \equiv 4 \bmod 25$
$2^3 \equiv 8 \bmod 25$
$2^6 \equiv 64 \equiv 14 \bmod 25$
$\equiv -11$

$2^{12} \equiv (-11)^2 \equiv 121 \bmod 25$
$\equiv 21$
$2^{13} \equiv 2 \cdot 21 \equiv 42 \equiv 17 \bmod 25$.
So $\boxed{N \equiv 17 \bmod 25}$.

    (c) From parts (a) and (b), deduce the last two digits (units digit and tens digit) of N.

From (a) $N = 4k$ for some k
From (b), $4k \equiv 17 \bmod 25$
$19 \cdot 4k \equiv 19 \cdot 17 \bmod 25$
$k \equiv (-6)(-8) \equiv 48 \equiv 23 \bmod 25$

Hence $N = 4 \cdot (23 + 25h) = 92 + 100h$
ie $N \equiv 92 \bmod 100$.

So the last two digits of N are $\boxed{92}$

13. (a) Let p be an *odd* prime (i.e. a prime besides 2), and k be a positive integer. Prove that if $a^2 \equiv 1 \pmod{p^k}$, then either $a \equiv 1 \pmod{p^k}$ or $a \equiv -1 \pmod{p^k}$.

Note the idea here is to mimic the proof of the "polynomials mod p" theorem.

$a^2 \equiv 1 \bmod p^k \iff (a+1)(a-1) \equiv 0 \bmod p^k$
$\iff p^k \mid (a+1)(a-1)$.

Now, since $a+1$ & $a-1$ differ by 2, and $p>2$, p can divide at most one of $(a+1)(a-1)$, and p^k is relatively prime to the other (since the only possible common prime factor is p).

Therefore, whichever of $a+1, a-1$ is divis. by p is in fact divis. by p^k. Hence

either $p^k \mid (a+1)$ or $p^k \mid (a-1)$

i.e. either $a \equiv -1 \bmod p^k$ or $a \equiv 1 \bmod p^k$

as desired.

(b) Find all integers a between 1 and 63 inclusive such that $a^2 \equiv 1 \pmod{64}$.

$64 = 2^6$, and $p=2$ so part (a) doesn't apply. Like in (a) we must have $64 \mid (a+1)(a-1)$, but now both $a+1$ & $a-1$ will be even. At most one is divis. by 4, however, so for 64 to divide $(a+1)(a-1)$, it is necessary (and sufficient) for 32 to divide one of $a+1, a-1$ (since 2 will automatically divide the other)

Therefore $a^2 \equiv 1 \bmod 64 \iff a \equiv \pm 1 \bmod 32$.

The possible a in $\{1, 2, \cdots, 63\}$ are $\boxed{1, 31, 33, \text{ and } 63}$

14. The number 2 is a primitive root modulo 29 (you may assume this without proof). If it is useful, you may use the modulo 29 multiplication table provided at the back of the packet.

(a) Prove $e_{29}(4) = 14$.

Observe that for $k = 1, 2, \cdots, 13$. we have

$4^k \equiv 2^{2k} \not\equiv 1 \bmod p$

since $0 < 2k < 28$ & 28 is the order of 2.

But for $k = 14$.

$4^{14} = 2^{28} \equiv 1 \bmod p$ (FLT. or using order of $2 = 28$).

So $4^1, \cdots, 4^{13} \not\equiv 1 \bmod p$ & $4^{14} \equiv 1 \bmod p$ $\Rightarrow$ 4 has order 14.

(b) State, with proof, a specific number $a \in \{1, \cdots, 28\}$ with order 7 modulo 29.

Let $\underline{a = 16}$.

Then $a = 2^4$. So $a^1, a^2, \cdots, a^6$ are $2^4, 2^8, \cdots, 2^{24}$

which are all $\not\equiv 1 \bmod 29$ since $e_{29}(2) = 28$,

but $a^7 = 2^{28} \equiv 1 \bmod 29$.

So $e_{29}(a) = 7$.

(c) Give an example of another primitve root modulo 29. You do not need to prove that your answer is correct; just state the number and how you obtained it.

Let $g = 8 = 2^3$.

Since $\gcd(3, 29-1) = 1$, this is a primitive root (proved in a homework problem).

Multiplication table modulo 29**:**

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	1	3	5	7	9	11	13	15	17	19	21	23	25	27
3	0	3	6	9	12	15	18	21	24	27	1	4	7	10	13	16	19	22	25	28	2	5	8	11	14	17	20	23	26
4	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
5	0	5	10	15	20	25	1	6	11	16	21	26	2	7	12	17	22	27	3	8	13	18	23	28	4	9	14	19	24
6	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
7	0	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3	10	17	24	2	9	16	23	1	8	15	22
8	0	8	16	24	3	11	19	27	6	14	22	1	9	17	25	4	12	20	28	7	15	23	2	10	18	26	5	13	21
9	0	9	18	27	7	16	25	5	14	23	3	12	21	1	10	19	28	8	17	26	6	15	24	4	13	22	2	11	20
10	0	10	20	1	11	21	2	12	22	3	13	23	4	14	24	5	15	25	6	16	26	7	17	27	8	18	28	9	19
11	0	11	22	4	15	26	8	19	1	12	23	5	16	27	9	20	2	13	24	6	17	28	10	21	3	14	25	7	18
12	0	12	24	7	19	2	14	26	9	21	4	16	28	11	23	6	18	1	13	25	8	20	3	15	27	10	22	5	17
13	0	13	26	10	23	7	20	4	17	1	14	27	11	24	8	21	5	18	2	15	28	12	25	9	22	6	19	3	16
14	0	14	28	13	27	12	26	11	25	10	24	9	23	8	22	7	21	6	20	5	19	4	18	3	17	2	16	1	15
15	0	15	1	16	2	17	3	18	4	19	5	20	6	21	7	22	8	23	9	24	10	25	11	26	12	27	13	28	14
16	0	16	3	19	6	22	9	25	12	28	15	2	18	5	21	8	24	11	27	14	1	17	4	20	7	23	10	26	13
17	0	17	5	22	10	27	15	3	20	8	25	13	1	18	6	23	11	28	16	4	21	9	26	14	2	19	7	24	12
18	0	18	7	25	14	3	21	10	28	17	6	24	13	2	20	9	27	16	5	23	12	1	19	8	26	15	4	22	11
19	0	19	9	28	18	8	27	17	7	26	16	6	25	15	5	24	14	4	23	13	3	22	12	2	21	11	1	20	10
20	0	20	11	2	22	13	4	24	15	6	26	17	8	28	19	10	1	21	12	3	23	14	5	25	16	7	27	18	9
21	0	21	13	5	26	18	10	2	23	15	7	28	20	12	4	25	17	9	1	22	14	6	27	19	11	3	24	16	8
22	0	22	15	8	1	23	16	9	2	24	17	10	3	25	18	11	4	26	19	12	5	27	20	13	6	28	21	14	7
23	0	23	17	11	5	28	22	16	10	4	27	21	15	9	3	26	20	14	8	2	25	19	13	7	1	24	18	12	6
24	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5
25	0	25	21	17	13	9	5	1	26	22	18	14	10	6	2	27	23	19	15	11	7	3	28	24	20	16	12	8	4
26	0	26	23	20	17	14	11	8	5	2	28	25	22	19	16	13	10	7	4	1	27	24	21	18	15	12	9	6	3
27	0	27	25	23	21	19	17	15	13	11	9	7	5	3	1	28	26	24	22	20	18	16	14	12	10	8	6	4	2
28	0	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1