Solutions for the Practice Final

1. **Ian and Nai play the game of todo, where at each stage one of them flips a coin and then rolls a die. The person who played gets as many points as the number rolled plus one if the coin came up heads, and the number rolled minus one if the coin came up tails. For example, if Ian gets heads and rolls a 3, he gets 4 points, whereas if Nai gets tails and rolls a 6, he gets 5 points.**

   (a) **What is the probability that a person gets 7 points in one turn?**

   First notice that the total number of possible outcomes in every turn is $2 \times 6 = 12$, 2 for the coin and 6 for the die. The only way for a person to get 7 is if the coin came up heads and the die 6. Thus the probability is $\boxed{1/12}$.

   (b) **Ian just made 3 points. What is the probability that Nai will get more points in his turn?**

   Nai wins if he makes $4, 5, 6$ or 7 points. The only ways for that to happen are $H-3$, $T-5$; $H-4$, $T-6$; $H-5$; $H-6$ and the probability is $\boxed{6/12 = 1/2}$.

   (c) **In the above situation, what is the probability that Nai will get the same number of points?**

   For Nai to get 3 points the possibilities are $H-2$ and $T-4$, and the probability is $2/12 = \boxed{1/6}$.

2. **Four standard 6-sided dice are rolled.**

   (a) **What is the probability that the sum of the values shown is 5?**

   An outcome of throwing 4 dice is a sequence of four numbers from 1 to 6; so the total number of possible outcomes is 6^4.

   The only way that four numbers between 1 and 6 have a sum of 5 is that one of them is a 2 and three of them are a 1. There are four choices for the position of the 2 among the four numbers, so there are four outcomes. The probability that the sum of the values shown is 5 is therefore $\boxed{\dfrac{4}{6^4}}$.

   (b) **What is the probability that all four dice show different values?**

   Again there are 6^4 outcomes. To get four different values, we need to count all sequences of four numbers between 1 and 6 with all numbers different. There are 6 possibilities for the first number, 5 for the second, 4 for the third and 3 for the last one. Therefore the probability that all four dice show different values is $\boxed{\dfrac{6 \cdot 5 \cdot 4 \cdot 3}{6^4}}$.

   (c) **What is the probability that only 1's, 2's and 3's occur but not all dice show the same value? (Note that not all three numbers have to occur, e.g. 2223 is a valid outcome.)**

   There are 6^4 possible outcomes. If only 1's, 2's and 3's are allowed, then there are 3 choices for each of the four positions (1, 2 or 3 for each one), so the total number of outcomes with only 1's, 2's and 3's is 3^4. We still need to subtract those outcomes where all four dice are equal (i.e. all 1, all 2 or all 3). Therefore the total number of favorable outcomes is $3^4 - 3$ and the final answer is $\boxed{\dfrac{3^4 - 3}{6^4}}$.

3. **Prof. Elkies is making bracelets for his nieces. Each bracelet has 23 beads, and each bead may be any of the three colors blue, pink, and purple.**

   (a) **How many possible bracelets are there?**
   We have 3 choices for each of 23 beads, so by the Multiplication Principle the total is $3 \times 3 \times 3 \times \ldots \times 3$ (23 factors) or $\boxed{3^{23}}$.

   (b) **Of those, how many use at least two different-colored beads?**
   Use the Subtraction Principle. If a bracelet does *not* use at least two different-colored beads, it must be all blue, all pink, or all purple: there are only 3 possibilities. Hence the number of bracelets that *do* use at least two different-colored beads is $\boxed{3^{23} - 3}$.

   (c) **One niece asks that her bracelet include at least one bead of each of the three available colors. How many such bracelets are there?**
   Again the Subtraction Principle, though a bit more work is required: in addition to the single-color bracelets, we must also eliminate those that use exactly two colors. Arguing as in the previous part, we see that for each pair of colors there are $2^{23} - 2$ bracelets that use just those two colors (and uses each of them at least once). Since there are three possible two-color pairs, that leaves $\boxed{3^{23} - 3(2^{23} - 2) - 3}$ bracelets that use all three colors (or equivalently $\boxed{3^{23} - 3 \times 2^{23} + 3}$).

   (d) **Another niece insists that more than half of her beads be purple, her favorite color. How many such bracelets are there?**
   To construct such a bracelet, we choose the number of purple beads, call it p, which must be at least 12; choose where to put the p purple beads, which can be done in $\binom{23}{p}$ ways; and then choose for each of the remaining $23 - p$ slots a blue or pink bead, which by the Multiplication Principle can be done in 2^{23-p} ways. Since p may be any of $12, 13, 14, \ldots, 21, 22, 23$, the total is

$$2^{11}\binom{23}{12} + 2^{10}\binom{23}{13} + 2^{9}\binom{23}{14} + \cdots + 2^{2}\binom{23}{2} + 2\binom{23}{1} + 1\binom{23}{0}$$

   (of course the final two terms can be written more simply as 2×23 and 1 respectively).

Remark: Since 23 is prime, you can check that your answer to the second part must be a multiple of 23. Can you see this directly? (One can give yet another proof of Fermat's theorem this way.)

By Fermat, $3^{22} \equiv 1 \bmod 23$, so $3^{23} - 3 = 3(3^{22} - 1) \equiv 0 \bmod 23$. To see this directly, group the non-monochromatic bracelets into sets of 23 by grouping each bracelet with all its rotations! Do you see how we are using the fact that 23 is prime in this argument?

4. **You are playing Scrabble$^{\text{TM}}$, and draw the letters EEESSTT.**

   (a) **In how many ways can you arrange these letters to form a 7-letter "word"?**
   Your 7 tiles comprise 3 E's, 2 S's, and 2 T's. Hence the number of rearrangements is the "trinomial coefficient" $\boxed{\binom{7}{3,2,2}} = \boxed{7!/(3!(2!)^2)}$. (As usual we encourage you to leave the answer in one of these symbolic forms; the numerical value here is 210.)

   (b) **If you choose one of these arrangements randomly, what is the probability that you will make one of the two actual words SETTEES and TESTEES that these letters form?**
   Two favorable outcomes out of $\binom{7}{3,2,2}$ equally likely outcomes makes the probability $\boxed{2 \;/\; \binom{7}{3,2,2}} = \boxed{2/\big(7!/(3!(2!)^2)\big)}$ (numerically, 1/105 or just under 1%).

(c) **If you choose one of the arrangements of your letters EEESSTT randomly, what is the probability of getting the three E's in a row (as in EEESSTT or SEEETTS, but not ESESETT or TSETSEE)?**

To count the "favorable" outcomes in this case, we regard EEE as a single "letter", and count the arrangements of one EEE, two S's, and two T's. The answer is $\binom{5}{1,2,2} = 5!/(1!(2!)^2)$ as before (you may of course omit the factor of $1! = 1$), and so the probability is $\boxed{\binom{5}{1,2,2}/\binom{7}{3,2,2}}$ (numerically, $30/210 = 1/7$ which comes to about 14.3%).

5. **Suppose a kindergarten class has 7 girls and 3 boys.**

(a) **How many ways are there to put the students in a line if we require that the first and last people in line are both girls?**

First, we choose a boy/girl template. The line must begin and end with a G, so there are 5 G's and 3 B's to fill the middle 8 slots. There are $\binom{8}{3}$ ways to arrange these, and thus there are $\binom{8}{3}$ boy/girl templates. For each template, we must then decide which particular girls and which particular boys to put in the slots. There are 7! ways to arrange the girls in the G slots, and 3! ways to arrange the boys in the B slots. Thus, there are $\boxed{\binom{8}{3} \cdot 7! \cdot 3!}$ ways to put the students in line.

(b) **Suppose that the class must be divided into two groups, with 5 of them going outside to recess and the other 5 staying inside to study math. How many ways are there to do this?**

We simply need to choose which 5 go out to recess; the rest stay in and study. So we just need to choose 5 students out of 10, and there are clearly $\boxed{\binom{10}{5}}$ ways of doing so.

(c) **Suppose that each of the two groups from the previous part must contain students of each gender. Now how many ways are there of putting the students into groups?**

We will use the subtraction principle. We already computed the total number of ways of dividing the students in the previous part, so now we need to compute the number of ways which aren't allowed. There are $\binom{7}{5}$ ways dividing the class in which the recess group is all girls; we just need to choose 5 of the 7 girls to go to recess. Similarly, there are $\binom{7}{5}$ ways dividing the class in which the math group is all girls. Note that these are the only ways we could have a group with only one gender, since there aren't enough boys to fill an entire group. Also, these two cases have no overlap, since it's impossible for the recess and math groups both to be composed of only girls. Thus, the total number of ways to divide the class such that each group contains students of each gender is $\boxed{\binom{10}{5} - 2\binom{7}{5}}$.

6. **Florian picks three cards at random out of a 52 card deck, records them, and returns them to the deck. Grigor does the same (he picks three cards at random out of the 52 card deck, and records them).**

(a) **What is the probability that at least one card will have been chosen by both Florian and Grigor?**

$$1 - \frac{49 \cdot 48 \cdot 47}{52 \cdot 51 \cdot 50}$$

.

(b) **What is the probability that none of Florian's cards are aces?**

$$\frac{48 \cdot 47 \cdot 46}{52 \cdot 51 \cdot 50}$$

.

7. (a) **Are there solutions to the equation**

$$22 = 23X + 21Y$$

in whole numbers (X, Y)**? If so, find** *two* **solutions** (X, Y)**.**
Since $1 = 23 \cdot 11 + 21 \cdot (-12)$ we can take $X = 22 \cdot 11 = 242$ and $Y = 22 \cdot (-12) = -264$. Also, we could subtract 210 from X and adding 230 to Y gives the solution $X = 32$ and $Y = -34$.

(b) **What is the least common multiple of** 96 **and** 162**?**
Since $96 = 3 \cdot 2^5$ and $162 = 2 \cdot 3^4$, the greatest common divisor of the two numbers is 6, so the least common multiple is $96 \cdot 162/6 = 2592$.

8. **Let** $c = \binom{24}{11}$**.**

(a) **Is** c **divisible by 17?**
We see, writing c as a fraction, that there is a 17 in the numerator, but not in the denominator. Since 17 is prime, this means that, $\boxed{\text{yes}}$, c is divisible by 17.

(b) **Is** c **divisible by 15?**
We know that c is divisible by 15 if and only if it is divisible by both 3 and 5. Further, we have that

$$c = \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}.$$

The numerator has five 3's (one each from 15, 21, and 24, and two from 18), and the denominator has four 3's. Thus c is divisible by 3. On the other hand, the numerator has two 5's, and the denominator also has two 5's. Thus c is not divisible by 5. We conclude that, $\boxed{\text{no}}$, c is not divisible by 15.

(c) **For what numbers** m **does the equation** $c \cdot x + 29y = m$ **have a solution (where, as usual, we mean a solution with** x **and** y **being whole numbers)?**
We know that this equation has a solution precisely when m is a multiple of the gcd of c and 29. We know that 29 is prime, and it is clear that c has no 29's in its prime factorization. Thus c and 29 are relatively prime, which means that their gcd is 1. It follows that the above equation has a solution for $\boxed{\text{any whole number m}}$.

9. (a) **Which is bigger,** 22^5 **or** $\binom{22}{17}$**?**
Writing $22^5 = 22 \cdot 22 \cdot 22 \cdot 22 \cdot 22$ and

$$\binom{22}{17} = \binom{22}{5} = \frac{22 \cdot 21 \cdot 20 \cdot 19 \cdot 18}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}$$

makes it clear that 22^5 is the bigger of the two numbers.

(b) **Is** $\binom{22}{17}$ **even or odd?**
Even.

(c) **Which prime numbers** p **bigger than** 11 **are divisors of the number** $\binom{22}{17}$**?**
19.

10. **In the first two parts of the following problems please write the answer as product of powers of prime numbers.**

(a) **Find the least common multiple A of the numbers from 1 to 10 (inclusive).**
The numbers from 2 to 10 can be written as $2, 3, 2^2, 5, 2 \times 3, 7, 2^3, 3^2, 2 \times 5$. We see that $A = 2^3 \times 3^2 \times 5 \times 7$.

(b) **Compute $\phi(10!)$.**
From the previous remark we see that

$$10! = 2^{1+2+1+3+1} \times 3^{1+1+2} \times 5^{1+1} \times 7 = 2^8 \times 3^4 \times 5^2 \times 7$$

Using the formula for the Euler ϕ-function we get

$$\phi(10!) = 2^7 \times 3^3 \times 5 \times (2-1)(3-1)(5-1)(7-1) = 2^{11} \times 3^4 \times 5.$$

(c) **How many numbers divide $\phi(10!)$ but not A?**
For the final part, let us compute

$$\gcd(A, \phi(10!)) = \gcd(2^3 \times 3^2 \times 5 \times 7, 2^{11} \times 3^4 \times 5) = 2^3 \times 3^2 \times 5$$

By the subtraction principle to find how many numbers divide $\phi(10!)$ but not A, we have to subtract from the number of the divisors of $\phi(10!)$ the number of the divisors of $\gcd(\phi(10!), A)$. We get the following answer :

$$(11+1)(4+1)(1+1) - (3+1)(2+1)(1+1) = 120 - 24 = \boxed{96}.$$

11. (a) **Given that 2 is a generator for arithmetic modulo the prime 53, how many square roots does 2 have modulo 53?**
$\boxed{\text{None}}$: a generator has no square roots. If x were a square root, we could write x as a power of the generator 2, say $x \equiv 2^a \bmod 23$. Then $2 = x^2 \equiv 2^{2a}$. But 2 is also 2^1, so (again since 2 is a generator) if $2^1 = 2^{2a}$ then $2a - 1$ is a multiple of $23 - 1 = 22$. This is impossible because $2a - 1$ is odd but 22 is even.
[If this analysis feels familiar, that's because it's essentially how we proved Legendre's formula, which says that a is has a square root modulo an odd prime p if and only if $a^{(p-1)/2} \equiv 1 \bmod p$. If you remembered this formula, you could also say simply that $2^{(53-1)/2}$ must be $-1 \bmod 53$ because 2 is a generator, so 2 cannot have a square root mod 53.]

(b) **How many square roots does 1 have modulo 51? Find them all.**
51 is the product of the distinct primes 3 and 17. Modulo an odd prime, the square roots of 1 are 1 and -1, and no others. So a square root of 1 mod 51 must be congruent to either 1 or -1 mod 3, and to either 1 or -1 mod 17. That's $2 \times 2 = 4$ possibilities, and by the Chinese Remainder Theorem each one yields a unique answer mod 51, so there are $\boxed{\text{four}}$ square roots. Two of them are of course 1 and -1. The others are congruent to $+1$ mod 3 and to -1 mod 17, or vice versa; using either Euclid or eyeballs we find that these are respectively 16 and $35 \equiv -16$. Hence the four roots are ± 1 and ± 16, that is $\boxed{1,\ 16,\ 35,\ \text{and}\ 50}$ mod 51.

(c) **How many square roots does 0 have modulo 49? Find them all.**
We did not discuss square roots of zero, and modulo non-primes at that. So we go back to the definition: find x mod 49 such that $x^2 \equiv 0 \bmod 49$, that is, such that x^2 is a multiple of 49. Since $49 = 7^2$, this amounts to requiring that x be a multiple of 7 (the easiest way to see this is to invoke unique factorization). There are $\boxed{\text{seven}}$ such multiples mod 49, namely $\boxed{0,\ 7,\ 14,\ 21,\ 28,\ 35,\ \text{and}\ 42}$.

12. (a) **Find all odd numbers n such that $\phi(n) = 6$. (Hint: Use Euler's theorem.)**

If n is an odd number, then n is relatively prime to 2 and if $\phi(n) = 6$, Euler's theorem tells us that $2^6 \equiv 1 \bmod n$. Equivalently, we see that n divides $2^6 - 1 = 63 = 9 \times 7$. Computing ϕ of the divisors of 63 we see that $n = 9$ or $n = 7$.

(b) **Find all numbers n such that $\phi(n) = 6$.**

If n is an even number such that $\phi(n) = 6$, then we can write it as $n = 2^a m$ $(a \geq 1)$with m being odd. Then $\phi(n) = 2^{a-1} \times \phi(m)$. The only possibilities are $a = 1$ and $\phi(m) = 6$ and $a = 2$ and $\phi(m) = 3$. Any odd number $m > 1$ will have an odd prime divisor q and then $\phi(m)$ will be divisible by $(q - 1)$ which is even. This shows that $\phi(m) = 3$ is not possible and we are left with $n = 2 \times 9$, 2×7.

(c) **For each of the composite numbers n such that $\phi(n) = 6$, find a witness for the fact that they are not prime.**

The numbers n such that $\phi(n) = 6$ are $7, 9, 14, 18$. Among them $9, 14, 18$ are not primes. We have that $2^8 \equiv 4 \bmod 9$, so 2 is a witness. We have $3^{13} \equiv (3^6)^2 \times 3 \equiv 3 \bmod 14$ which shows that 3 is a witness $\bmod 14$. For 18 we see that 5 works - if 5 was not a witness, then $5^{17} \equiv 1 \bmod 18$ and $5^{18} \equiv 5 \bmod 18$, but using Euler's theorem again, $5^{18} = (5^6)^3 \equiv 1 \bmod 18$.

13. (a) **Find a generator G for arithmetic modulo the prime 23. Make a table of x and G^x for each $x = 0, 1, 2, \ldots, 21$.**

You have ten correct choices for G; each one will lead you to the same answer in the rest of the problem (except of course for G^{219}, and possibly for the choice of square root of 6). The easiest choices to calculate with are probably $G = -2$ (a.k.a. 21) and $G = 5$. We illustrate with $G = -2$. The table is

x	0	1	2	3	4	5	6	7	8	9	10
G^x	1	21	4	15	16	14	18	10	3	17	12

x	11	12	13	14	15	16	17	18	19	20	21
G^x	22	2	19	8	7	9	5	13	20	6	11

Note that the middle power G^{11} is -1, as we knew it must be.

(b) **Use your table to quickly compute each of the following mod 23:**

i. 11×13

ii. $11/13$

iii. 11^{13}

iv. G^{219}

Find 11 and 13 in the G^x row of the table: $11 \equiv G^{21}$ and $13 \equiv G^{18}$. Thus

$$11 \times 13 \equiv G^{18+21} = G^{39} \equiv G^{17} \equiv 5$$

(using $G^{22} \equiv 1$ in the next-to-last step), and likewise

$$11/13 \equiv G^{21-18} = G^3 \equiv 15.$$

As for 11^{13}, that is $(G^{21})^{13} = G^{21 \times 13}$; here it is easier to write $11 \equiv G^{21} \equiv G^{-1}$, making $11^{13} \equiv G^{-13} \equiv G^{22-13} = G^9 \equiv 17$. Finally, since $219 = 10 \times 22 - 1$, we have $G^{219} \equiv G^{10 \times 22 - 1} = (G^{22})^{10} G^{-1}$, in which the first factor $(G^{22})^{10}$ is 1 by Fermat (since $G^{22} \equiv 1$), while $G^{-1} = G^{21}$ can be found on our table; having chosen $G = -2$, we get $G^{219} \equiv 11$.

(c) **Use your table to find a square root of** 6 mod 23**. Check your work by verifying directly that it is in fact a square root.**

Find 6 in the G^x row: $6 \equiv 2^{20}$. So a square root is $2^{20/2} = 2^{10}$, which again we locate in the table: it's 12. Check: $12^2 - 6 = 144 - 6 = 138$, which indeed is a multiple of 23 (namely 6×23).

14. **Let** p **be one of the primes** $3, 5, 7, 11, 13$**.**

(a) **For which** p **does** 2 **have a square root** (mod p)**?**

To check whether 2 has a square root mod p we have to compute $2^{\frac{p-1}{2}} \bmod p$.

$$2^1 \equiv -1 \bmod 3, \text{ — 2 does not have a square root mod 3}$$

$$2^2 \equiv -1 \bmod 5, \text{ — 2 does not have a square root mod 5}$$

$$2^3 \equiv 1 \bmod 7, \text{ — 2 has a square root mod 7}$$

$$2^5 \equiv -1 \bmod 11, \text{ — 2 does not have a square root mod 11}$$

$$2^6 \equiv -1 \bmod 13, \text{ — 2 does not have a square root mod 13}$$

(b) **For each one for the possibilities for** p **find a generator** (mod p)**.**

Computing $1, 2^1, 2^2, \ldots, 2^{p-2} \bmod p$ for $p = 3, 5, 11, 13$ we see that 2 is a generator. It is easy to see that 3 for example is a generator mod 7.

15. **Suppose we are given that** 3 **is generator** (mod 17)**.**

(a) **How many numbers** (mod 17) **have a cube root** (mod 17)**?**

Because 3 is relatively prime to 16, any number has a unique cube root mod 17.

(b) **Find all solutions to** $x^3 \equiv 3$ (mod 17)**.**

Let x be the cube root of 3 mod 17. Then using the fact that 3 is a generator mod 17 we can write $x \equiv 3^u \bmod 17$ for some u, such that $3u \equiv 1 \bmod 16$. We see that $u = 11$, works which gives

$$x \equiv 3^{11} \equiv 27 \times (81)^2 \equiv 10 \times (-4)^2 \equiv 7 \bmod 17$$

(c) **Find all pairs** x**,** y **of integers** (mod 17)**, where neither one is allowed to be zero, such that** $x^4 + y^4 \equiv -1$ (mod 17)**.**

For the last part, let us find all 4-th powers mod 17. They are all of the form $3^{4k} = (3^4)^k \bmod 17$ for some k. First compute $3^4 \equiv -4 \bmod 17$. The 4-th powers mod 17 are $0, 1, -4, (-4)^2 \equiv -1$. The only way the sum of two 4-ths can be -1 is one of them to be zero and the other -1. Since we don't allow either one to be zero, it follows that there are no such pairs x and y.

16. **Express the answer to these numerical questions mod** 23 **in terms of the congruence classes**

$$\{0, 1, 2, 3, \ldots, 22\}.$$

(a) $22^3 \pmod{23}$

We see that $22 \equiv -1 \pmod{23}$, and thus

$$22^3 \equiv (-1)^3 \equiv -1 \equiv \boxed{22} \pmod{23}.$$

(b) $3^{22} \pmod{23}$

We know that 23 is prime, and thus Fermat's theorem says that $3^{22} \equiv \boxed{1} \pmod{23}$.

(c) $3^{33} \pmod{23}$ **(Hint:** $3^3 \equiv 2^2 \pmod{23}$.**)**

If we start from the hint, then raising both sides to the 11th power gives $3^{33} \equiv 2^{22} \pmod{23}$. But by Fermat's theorem, $2^{22} \equiv 1 \pmod{23}$. We conclude that $3^{33} \equiv \boxed{1} \pmod{23}$.

17. **Alice and Bob must communicate via an insecure channel, but have no real reason to keep anything they say private. Nevertheless, veterans of QR28 that they are, Bob proposes that they practice the public key code method taught in QR28, but for a choice of ridiculously small (odd) prime numbers P and Q. That is, Bob will choose two primes P and Q and form the product $N = P \cdot Q$. He will then choose a number k *for which the code will actually work,* and will send to Alice the numbers N and k. As usual, he will then ask Alice to encode her message as a number a and "publish" (that is, send back to him via the insecure channel) the quantity a^k modulo N. For some curious reason, Bob is bent on choosing $k = 15$. What are the smallest distinct prime numbers P and Q that he can use to manufacture the $N = P \cdot Q$ he will be sending to Alice?**

$P = 5$ and $Q = 3$ because this is the choice of smallest primes such that k is relatively prime to $\phi(P \cdot Q)$. Of course, it would be ridiculous for him to choose such low primes...

18. **Alice and Bob wish to exchange messages using the RSA encryption scheme. First, Bob chooses $p = 11$ and $q = 19$ as his secret, "large" primes. He publishes their product, $N = 209$, and he also chooses and publishes $k = 23$ as the encryption exponent.**

(a) **If Alice wishes to send the message 35 to Bob, what should she send?**

Alice encrypts a message by raising it to the kth power (mod N). Thus, in this case, she should compute $35^{23} \pmod{209}$. We have

$$\begin{aligned} 35^2 &\equiv 1225 \equiv 180 \equiv -29 \\ 35^4 &\equiv 841 \equiv 5 \\ 35^8 &\equiv 25 \\ 35^{16} &\equiv 625 \equiv 207 \equiv -2 \end{aligned}$$

where all of these equivalences are taken (mod 209). Thus we have

$$35^{23} \equiv 35^{16} \cdot 35^4 \cdot 35^2 \cdot 35 \equiv -2 \cdot 5 \cdot -29 \cdot 35 \equiv -10 \cdot 30 \equiv -300 \equiv 118 \pmod{209}.$$

Thus Alice should send $\boxed{118}$ to Bob.

(b) **If Bob receives the transmission 5, what was Alice's message?**

Bob decrypts a message by taking its kth root (mod N). In this case, that means he should compute $5^{1/23} \pmod{209}$. We know that $209 = 11 \cdot 19$, and thus $\phi(209) = 180$. The Euclidean algorithm gives

$$\begin{aligned} 180 &= 7 \cdot 23 + 19 \\ 23 &= 19 + 4 \\ 19 &= 4 \cdot 4 + 3 \\ 4 &= 3 + 1, \end{aligned}$$

and running it backwards, we have

$$\begin{aligned}1 &= 4 - 3\\ 1 &= 4 - (19 - 4 \cdot 4) = -19 + 5 \cdot 4\\ 1 &= -19 + 5(23 - 19) = 5 \cdot 23 - 6 \cdot 19\\ 1 &= 5 \cdot 23 - 6(180 - 7 \cdot 23) = -6 \cdot 180 + 47 \cdot 23.\end{aligned}$$

Thus $5^{1/23} \equiv 5^{47} \pmod{209}$. Successive squaring gives

$$\begin{aligned}5^2 &\equiv 25\\ 5^4 &\equiv 625 \equiv 207 \equiv -2\\ 5^8 &\equiv 4\\ 5^16 &\equiv 16\\ 5^{32} &\equiv 256 \equiv 47\end{aligned}$$

where all of these equivalences are taken (mod 209). Thus we have

$$5^{47} \equiv 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \cdot 5 \equiv 47 \cdot 4 \cdot -2 \cdot 25 \cdot 5 \equiv -21 \cdot -41 \equiv 861 \equiv 25 \pmod{209}.$$

We conclude that Alice's message was $\boxed{25}$.
In this case, it's easy to check our answer. We wish to confirm that $25^{23} \pmod{()209}$ really is 5 (mod 209). Since $25 = 5^2$, we see that $25^{23} = 5^{46}$, and therefore

$$25^{23} \equiv 5^{46} \equiv 5^{47}/5 \equiv 25/5 \equiv 5 \pmod{209},$$

since we've already computed $5^{47} \pmod{209}$ above, and we know division by 5 is allowed (mod 209). Thus our answer is correct.

19. **Alice and Bob wish to use the password scheme we've discussed. They choose 23 as their prime and 7 as a generator for arithmetic** (mod 23)**. Alice chooses 5 as her secret exponent, and then she publishes 17. Bob chooses 8 as his secret exponent and publishes 12. What is their password?**

Their password is $7^{5 \cdot 8} \pmod{23}$. Of course, neither one of them computes it in that way. Alice computes the password by doing $12^5 \pmod{23}$, and Bob computes it by doing $17^8 \pmod{23}$. These all give the same answer, although doing the computation the way Alice or Bob would is easier than computing $7^{5 \cdot 8} \pmod{23}$ directly. We will compute $12^5 \pmod{23}$, since it has the smallest exponent. We have

$$\begin{aligned}12^2 &\equiv 144 \equiv 6\\ 12^4 &\equiv 36 \equiv -10\end{aligned}$$

where all of these congruences are taken (mod 23). Thus we have

$$12^5 \equiv 12^4 \cdot 12 \equiv -10 \cdot 12 \equiv -120 \equiv 18 \pmod{23}.$$

We conclude that their password is $\boxed{18}$.

20. **Compute** $9^{\left(4^{163}\right)} \pmod{99}$**.**

We might be tempted to use Euler's theorem, except that 9 and 99 are not relatively prime, and therefore Euler's theorem doesn't apply. Instead, we can use the Chinese remainder theorem.

We start by computing $9^{\left(4^{163}\right)} \pmod 9$ and $9^{\left(4^{163}\right)} \pmod{11}$, since $99 = 9 \cdot 11$ and 9 and 11 are relatively prime. Since $9 \equiv 0 \pmod 9$, it's obvious that $9^{\left(4^{163}\right)} \equiv 0 \pmod 9$.

Next, we compute $9^{\left(4^{163}\right)} \pmod{11}$. Here, we can use Fermat's theorem, which tell us that, if $x \equiv 4^{163} \pmod{10}$, then $9^{\left(4^{163}\right)} \equiv 9^x \pmod{11}$. Thus we want to compute x. Again, 4 and 10 aren't relatively prime, so we can't use Euler's theorem. Nonetheless, successive squaring shows that

$$\begin{aligned} 4^2 &\equiv 6 \pmod{10} \\ 4^4 &\equiv 6 \pmod{10}, \end{aligned}$$

which means that every even power of 4 will be $6 \pmod{10}$. So

$$x \equiv 4^{163} \equiv 4^{162} \cdot 4 \equiv 6 \cdot 4 \equiv 4 \pmod{10}.$$

This means that

$$9^{\left(4^{163}\right)} \equiv 9^4 \equiv 81^2 \equiv 4^2 \equiv 5 \pmod{11}.$$

The Chinese remainder theorem now tells us that $9^{\left(4^{163}\right)} \pmod{99}$ is the unique congruence class (mod 99) which is congruent to $0 \pmod 9$ and to $5 \pmod{11}$. We could use the Euclidean algorithm to do this, but in this case it's probably easier just to guess a solution. The first few numbers which are congruent to $5 \pmod{11}$ are 5, 16, and 27. At this point we stop, because 27 is divisible by 9 and thus is also $0 \pmod 9$. We conclude that $9^{\left(4^{163}\right)} \equiv \boxed{27} \pmod{99}$.

21. **A number x between 1 and 30, inclusive, is chosen at random.**

    (a) **What is the probability that x is a generator in arithmetic modulo 31?**
    We know that for any odd prime p there are $\phi(p-1)$ generators for arithmetic mod p. Here $p = 31$ (check that it is indeed prime) and $p - 1 = 30 = 2 \times 3 \times 5$, so the Euler ϕ function of 30 is

    $$(2-1) \times (3-1) \times (5-1) = 1 \times 2 \times 4 = 8.$$

    So, we have 8 favorable outcomes out of 30 equally likely outcomes, for a probability of $\boxed{8/30}$.

    (b) **What is the probability that x has a fourth root modulo 31?**
    This and the next problem are most easily done by writing all the nonzero numbers mod 31 as powers of some generator G (you can use $G = 3$, but the choice of G doesn't matter here). So, $x = G^a$ for some a mod 30, and x as a fourth root, call it $y = G^b$, if and only if $a \equiv 4b$ mod 30 for some b mod 30. That is, a must be a "combo" of 4 and 30. As we know, this means that a is a multiple of $\gcd(4, 30) = 2$. In plain English, a must be even. If we choose a mod 30 randomly, the probability that it is even is clearly $\boxed{1/2}$ (or equivalently $\boxed{15/30}$ if you insist).

    (c) **What is the probability that x is a square but not a cube modulo 31?**
    Here a must be a multiple of 2 but not of 3 (since $\gcd(2, 30) = 2$ and $\gcd(3, 30) = 3$. Of the 15 multiples of 2, the multiples of 3 are precisely the multiples of 6, of which there are $30/6 = 5$ in arithmetic mod 30. Subtracting, we find $15 - 5 = 10$ favorable outcomes, for a probability of $\boxed{10/30} = \boxed{1/3}$.

22. (a) **Find generators modulo each of the following prime numbers: 5, 7 and 11.**

First we try whether 2 is a generator for each of these moduli. We find that it works for 5 and 11, but not for 7 (because $2^3 \equiv 1 \pmod 7$). But for 7 it is easy to check that 3 works as generator.

Here are the tables of powers in each case:

e	1	2	3	4
$2^e \bmod 5$	2	-1	-2	1

e	1	2	3	4	5	6
$3^e \bmod 7$	3	2	-1	-3	-2	1

e	1	2	3	4	5	6	7	8	9	10
$2^e \bmod 11$	2	4	-3	5	-1	-2	-4	3	-5	1

(b) **Using your answer to (a), or otherwise, find all the squares mod 11.**

Using the fact that 2 is a generator mod 11, it follows that the squares mod 11 are precisely 2^e for even numbers e (and 0 is also a square). The reason is that any non-zero number is 2^x for some x (because 2 is a generator) so if it is squared it becomes 2^{2x} and $2x$ is even. On the other hand, any 2^{2x} is a square: it is 2^x squared. Why can't 2^f be a square when f is odd? Well, if it is then it equals 2^{2x} for some whole number x and so $2x \equiv f \pmod{10}$ (because 2 is a generator). But an even number ($2x$) and an odd number (f) can never differ by a multiple of 10 (by the 2/3-principle)!

So the answer is (from the table): $\boxed{4, 5, -2, 3, 1, \text{and } 0}$.

(A different method would be to just square out all numbers $0, 1, \ldots, 10$ modulo 11.)