QUANTUM ADVANTAGES ON FACTORIZATION PROBLEM

Xingjian Wu, Yiyang Zeng, Junlin Song, Hongjin Wang

Department of Computer Science, Columbia University

ABSTRACT

As quantum computing gradually comes to maturity, people are getting concerned if quantum computing can easily decipher any data encrypted in large-number factorization based systems with quantum advantages, thus ruin the entire Internet by destroying all online-safety. Although it does not seem a nightmare that would come true in the near future, different approaches to the factorization problem, the key to major modern world asymmetric encryption techniques, have been studied and implemented based on quantum computing for a long time.

In this paper, we are to introduce four different methods of quantum factorization and their state-of-the-art results. Subsequently we manage to extend the ability of Grover's algorithm on factorization by factorizing the number 9975814637 with 2 qubits implemented on IBM Quantum Experience, and conduct fidelity check to ensure reliability of test result. Result proves the success of our attempt: we observe good agreement between experimental and theoretical results with high fidelity. At last we will discuss the result, limitation of Grover's algorithm and as well as impact of quantum factorization on encryption.

Index Terms**—** Quantum Computing, Grover's Algorithm, Factorization, Encryption

1. INTRODUCTION

The ultimate goal of encryption is to ensure confidentiality, integrity, availability, and authenticity of data and protect it from attackers. Modern society mainly uses two sets of encryption systems (and also their hybrid), i.e. private-key system, and public-key system. Although private-key resembles people's imagination toward encryption, the existing state of Internet makes it impossible to dominate the market. With certain advantages from its property, public-key system has been incredibly commercially successful. It is a mature system whose safety is guaranteed by several NP-hard problems. Although generally not regarded as a NP-hard problem, factorization performed on classical computers still requires innumerable operations, rendering it as the guarantee for cryptography techniques such as RSA [1]. However, factorization problem is now posed under fatal threat by quantum computing.

Traditionally, operations taken to factoring a number of n digits grows exponentially to n in classical context, such as the approach described in [2] realized factorization in $O(2^{n^{1/3}})$ steps. Computation complexity needed in classical computers lays the foundation of impenetrableness of encryption. Quantum methods, in contrast, requires only polynomial time. Up till today there are four main methods of factorization in quantum computing: Shor's algorithm, Grover's algorithm, adiabatic quantum computation, and quantum annealing.

Shor's algorithm has been proven to theoretically allow a quantum computer to factor the same numbers with exponential speedup [3]. It works by reducing the factorization problem to the order-finding problem: first to determine the period of the function $f(x) = a^x \bmod N$, where a is a randomly chosen small number with no factors in common with N; from this period, number-theoretic techniques can be used to factor N with high probability.

Grover's algorithm takes another approach. Given an unsorted list of N elements, Grover's algorithm can find a target element with $O(\sqrt{N})$ operations, whereas a classical algorithm requires $O(N)$ operations. [4] proposed a generalized quantum search algorithm that searches M marked states from an arbitrary distributed N-item quantum database with a zero theoretical failure rate.

Quantum adiabatic computations lies on he basis of quantum adiabatic theorem: a quantum system remains in its instantaneous eigenstate if the system Hamiltonian varies slowly enough and if there is a gap between this eigenvalue and the rest of the Hamiltonian's spectrum, which proved to be equivalent to the conventional circuit model. [5] claims the method offers lower sensitivity to some perturbations and thus improved robustness against errors due to dephasing, environmental noise and some unitary control errors.

Quantum annealing is a variant of quantum adiabatic computations. [6] introduced an approach based on a direct mathematical transformation of the factorization problem to an Ising Hamiltonian, which can be realized using currently available quantum processors, as well as a modified multiplication method that reduces the range of the coefficients in the cost function without increasing the number of qubits required to account for hardware constraints.

Despite the fact that Shor's algorithm is the earliest and best-studied way of quantum factorization, it has not gone far in terms of factoring large numbers in its 20-year lifespan. Until 2012 the largest number factored using Shor's algorithm was only 21 [2], which surpasses the old record 15 published in 2001 [7]. Furthermore, above mentioned factorization were not genuine implementations of Shor's algorithm because they relied on prior knowledge of the answer to the factorization problem being solved in the first place, "(there is) danger in 'compiled' demonstrations of Shor's algorithm. To varying degrees, all previous factorization experiments have benefited from this artifice." [8].

Xu's research [9] presented a realization of an improved adiabatic factoring algorithm based on a liquid crystal nuclear magnetic resonance quantum processor with dipole-dipole couplings. They factored the number 143 with two-bit input. A later article [3] claimed that the Nuclear Magnetic Resonance (NMR) experiment by Xu actually factored an entire class of integers, where the largest number factored is $56153 = 233 \times 241$. Another paper [10] improved the system to three-bit input NMR and solved factorization of 551.

As opposed to performing factorization with genuine qubits, Jiang et al. factorized 376289 using 94 logical qubits, tested using the D-Wave 2000Q for finding an embedding and determining the prime factors for a given composite number [6]. In the paper they claimed that the resource-efficient method uses $O(\log_2 N)$ binary variables, or logical qubits, for finding the factors of an integer N.

The most astonishing claim for quantum-related factoring is based on Grover's algorithm. [11] solved $4088459 = 2017 \times 2027$ using 2 qubits (per their measure) of IBM quantum processors with 5-qubit and 16-qubit, with an optimal version of classical algorithm/analytic algebra. This is the largest claim for quantum factorization up to date.

Enlightened by the success of Dash, et al. [11] and with the aid of IBM Quantum Experience, we decided to broaden the scope of Grover's algorithm in quantum factorization and conclude whether present quantum computing techniques have posed threat towards the cornerstone of modern world encryption.

2. METHOD

2.1. Generalized Grover's algorithm

Here we used a generalized Grover's algorithm [4] to solve the factorization problem. The algorithm can find the target states with a zero theoretical failure rate. The algorithm is stated as the following:

Consider searching M marked states from an arbitrary distributed $N-$item quantum database. The initial state of the quantum database is prepared in

$$|\phi_0\rangle = a_0|0> + a_1|1\rangle + ... + a_{N-1}|N-1\rangle$$

where $a_0, a_1, ...a_{N-1}$ are some arbitrary complex numbers. Suppose $|\tau\rangle$ and $|c\rangle$ respectively represent the normalized state sum over all the marked states and all the non-marked states.

$$|\tau\rangle = \sqrt{\frac{1}{\sum_{i=\tau_1^{\tau_M}}}}(a_{\tau_1}|\tau_1\rangle + a_{\tau_2}|\tau_2\rangle + ... + a_{\tau_M}|\tau_M\rangle)$$

$$|c\rangle = \sqrt{\frac{1}{\sum_{i\neq\tau}|a_i|^2}}(\sum_{i\neq\tau} a_i|i\rangle)$$

Then we can express the database $|\phi_0\rangle = \sin\beta|\tau\rangle + \cos\beta|c\rangle$ The following is the quantum search subroutines to the initial state subroutine.

- Perform a conditional shift $e^{i\phi}$to the M target states. The value of ϕ is calculated by

  $$\phi = 2\arcsin(\frac{\sin\frac{\pi}{4J+2}}{\sin\beta})$$

  where J is the number of iterations that find the M marked items
- Perform a n-qubit oeration $U^\dagger$, where U transforms the n-qubit $|0\rangle$ state to $|\psi_0\rangle$ state.
- Perform a conditional phase shift $e^{i(\psi+\pi)}$ to $|0\rangle$ state and a conditional phase shift $e^{i\pi}$ to all the other basis states.
- Perform the n-qubit transformation U

2.2. Factorization to searching

A factorization problem is formulated as following: we seek to find out the prime factors p and q of an odd composite number $N = p \times q$. The binary form of p, q can be denoted as $\{1p_mp_{m-1}...p_2p_11\}$ and $\{1p_np_{n-1}...p_2p_11\}$ respectively. Then we can reduce the factorization problem into a set of equations in variables $\{p_i\}$ and $\{q_j\}$. This is because if $p_i + q_j = z, \quad z \in \{0, 2\}$, then $p_i = q_j = 0$ if $z = 0$ amd $p_i = q_j = 1$ if $z = 2$.

Starting from a simple case where $m = n$. Consider $N = 4088459 = 2017 \times 2027$. The prime factors of the number have the same number of digits. Then the factorization problem can be reduced to following

$$\begin{aligned}
&p_i = q_j = 0; i \in \{2, 4\}\\
&p_i = q_j = 1; i \in \{5, 6, 7, 8, 9\}\\
&p_1 + q_1 = 1\\
&p_3 + q_3 = 1\\
&p_1q_3 + p_3q + 1 = 0
\end{aligned}$$

The equation set where $i = 1, 3$ can be further reduced into

$$q_1 + q_3 - 2q_1q_3 = 0$$

Then we can use 2 quantum state to represent the solutions here. $|00\rangle$ means $p_1 = p_3 = 0$, $|11\rangle$ means $q_1 = q_3 = 1$. Using the generalized Grover algorithm above, we are searching the 2 target states from a quantum database.

3. RESULTS

For the result part, we attempt to demonstrate the procedure to factorize number **9975814637**. We solve this problem by translating it into Grover algorithm target, and apply a quantum circuit which only requires two qubits.

From the previous part of this report, it is clear that in order to translate a factorization problem into a problem which is solvable using Grover algorithm, certain limits should be applied onto the number. The prime number 9975814637 could be factorized into two large prime numbers 99877 and 99881.

The binary value of 99877 is 11000011000100101, and the binary value of 99881 is 11000011000101001. They all have 17 digits of binary values and both starts and ends with 1. They have two digits different from each other, which are the third and the fourth digits – $p_{34-99877} = 01$ and $q_{34-99881} = 10$.

The two-digit difference infoms that a two qubit Hamiltonian should be used to factorize $N = 9975814637$. Because all other variables where $p_i = q_i$ would be resolved during the simplification process. Hence, the solution is encoded in the 2 ground states of the 2 qubit Hamiltonian.

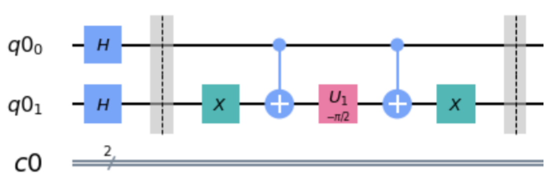

FIG. 1. Circuit part a

Figure 1 shows the first part of the quantum circuit. The first two Hadamard (H) Gates are the init part of every Grover algorithm circuit.

After the barrier line is the implementation for $e^{i(\sigma_z^1 \bigotimes \sigma_z^2)\frac{\theta}{2}}$, which is a simplification form to simulate $e^{-i\hat{H}\theta}$ on the system. The operation $e^{-i\hat{H}\theta}$ could be expressed as $e^{-i\hat{H}\theta} = e^{-iI_2\frac{\theta}{2}} e^{i(\sigma_z^1 \bigotimes \sigma_z^2)\frac{\theta}{2}}$ where the operation $e^{-iI_2\frac{\theta}{2}}$ is simply to introduce a global phase of $\frac{\theta}{2}$ to the system and carries no physical significance, so we ignore it in the implementation.

The operation $e^{i(\sigma_z^1 \bigotimes \sigma_z^2)\frac{\theta}{2}}$ in the implementation is expressed as the product of multiple unitary gates.

Two Pauli X gates, upon evaluating the Hamiltonian, conditionally shift phase to $|01\rangle$ and $|10\rangle$ states instead of $|00\rangle$ and $|11\rangle$ states.

Overall, the action of this part of the circuit is to conditionally introduces a phase shift of θ angle only to the ground states of $\hat{H}$ instead of other basis states, that encodes solution into the oracular part. Hence, our required "solution" states have been marked as required for the quantum search algorithm.

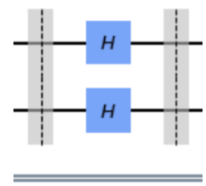

FIG. 2. Circuit part b

In the second step shown in figure 2, we apply the $U^\dagger$, which is the inverse operation of U such that $U|01\rangle = |\phi_0\rangle$, in order to compensate the previously required marking process that transformed qubits into 2-qubit equal superposition states.

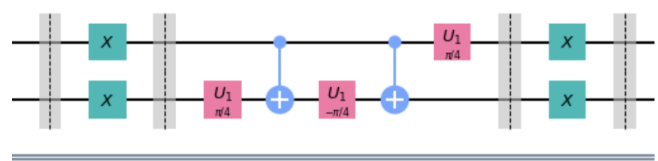

FIG. 3. Circuit part c

In the third part (figure 3), we implement to satisfy our amplitude amplification purpose that only targeted states would be applied phase shift $e^{i\theta}$, and leave other basis states unchanged.

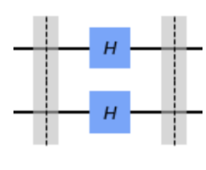

FIG. 4. Circuit part d

Finally, apply U to obtain an equal superposition of the marked states only. In this case, the value of θ must be $\frac{\pi}{2}$.

The circuit ends with two measurement gates, that separately translate output of two qubit to two classical bit registers.

The choice of θ depends on the choice of ϕ where in our case, $\phi = \frac{\pi}{4}$, and θ is obtained from the formula [4]:

$$\theta = 2sin^{-1}(\frac{sin\frac{\pi}{4j+2}}{sin\phi})$$

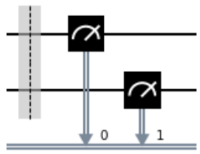

FIG. 5. Circuit part e

where j is the minimum number of iterations required to separate marked states with certainty.

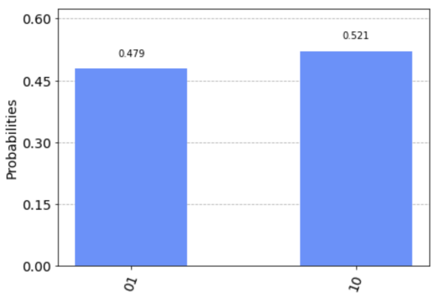

FIG. 6. Ideal circuit result

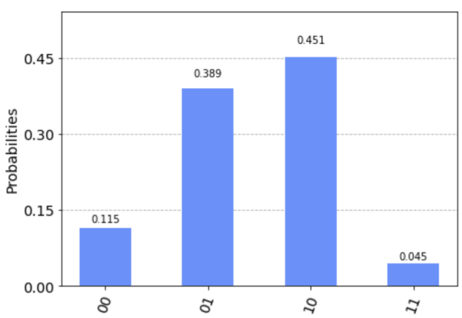

FIG. 7. Experimental circuit result

Figure 6 shows the result obtained from qasm_simulator background, with default 1024 shots. And Figure 7 shows the result obtained from real quantum computer with 8192 shots.

Both results shows that the circuit receives answers 01 and 10 with highest possibilities. Since 01 and 10 are the two different digits in binary form of 99877 and 99881, it is safe to conclude that Grover algorithm has successfully helped us to solve the factorization problem.

Fidelity quantifies the closeness of the experimentally obtained quantum states to the final state of the system in the ideal case. To calculate the fidelity of the circuit, we need to find both theoretical and experimental density matrix:

$$F(\rho^T, \rho^E) = Tr(\sqrt{\sqrt{\rho^T}\rho^E\sqrt{\rho^T}})$$

In theory, the final state obtained after the circuit is executed should be $|\Phi\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$. Thus the theoretical density matrix is:

$$\rho^T = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

As one may notice from the circuit, that it not only solves the factorization problem of $N = 9975814637$, but all numbers sharing the pattern that it could be divided into two odd prime numbers where the two prime numbers have the same length in binary form, and differs only two digits in binary form. And also the two different digits must be $\{01\}$ in one prime number and $\{10\}$ in the other.

This observation extends the use of circuit to all number satisfying the requirement, and based on our research, there are 41654 numbers in range from 5 to 10^{10}.

A excerpt of numbers can be found in the Appendix for reference.

4. DISCUSSION

Grover's algorithm uses amplitude amplification to find the answer, where different answers amplified require different circuits.Although it seems like "going in circle" that in order to solve the problem we need to know the answer first, the logic holds true generally to all oracular algorithms including Grover's. Essentially the answer is only needed to construct the oracle part of the circuit, whereas the rest of the circuit is always the same. It is not guaranteed that we may know the answer in constructing the oracle as an individual: either another party makes the oracle and it becomes a two-player-game, or the oracle is a function such as SAT and we do not know the satisfying set even though we know how to check if an input is satisfying.

Notably, there has emerged a relatively novel idea of post-quantum security, such as SPHINCS and McBits, proves to ensure encryption in the context of quantum computers. Post-quantum algorithms avoid acceleration brought by quantum algorithm such as Grover's and make use of problems to which Grover's algorithm does not offer an easy solution. Even though that does not mean there is no other algorithm that solves them, or even that there is no way to use Grover's for them, it still offers a solution to the problem of encryption in the presence of an emerging and promising field.

5. REFERENCES

[1] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[2] Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L O'brien, "Experimental realization of shor's quantum factoring algorithm using qubit recycling," *Nature photonics*, vol. 6, no. 11, pp. 773–776, 2012.

[3] Nikesh S Dattani and Nathaniel Bryans, "Quantum factorization of 56153 with only 4 qubits," *arXiv preprint arXiv:1411.6758*, 2014.

[4] Yang Liu, "An exact quantum search algorithm with arbitrary database," *International Journal of Theoretical Physics*, vol. 53, no. 8, pp. 2571–2578, 2014.

[5] Xinhua Peng, Zeyang Liao, Nanyang Xu, Gan Qin, Xianyi Zhou, Dieter Suter, and Jiangfeng Du, "Quantum adiabatic algorithm for factorization and its experimental implementation," *Physical Review Letters*, vol. 101, no. 22, Nov 2008.

[6] Shuxian Jiang, Keith A. Britt, Alexander J. McCaskey, Travis S. Humble, and Sabre Kais, "Quantum annealing for prime factorization," 2018.

[7] Lieven MK Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S Yannoni, Mark H Sherwood, and Isaac L Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[8] John A Smolin, Graeme Smith, and Alexander Vargo, "Oversimplifying quantum factoring," *Nature*, vol. 499, no. 7457, pp. 163–165, 2013.

[9] Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, and Jiangfeng Du, "Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system," *Physical review letters*, vol. 108, no. 13, pp. 130501, 2012.

[10] Soham Pal, Saranyo Moitra, VS Anjusha, Anil Kumar, and TS Mahesh, "Hybrid scheme for factorisation: Factoring 551 using a 3-qubit nmr quantum adiabatic processor," *Pramana*, vol. 92, no. 2, pp. 26, 2019.

[11] Avinash Dash, Deepankar Sarmah, Bikash K Behera, and Prasanta K Panigrahi, "Exact search algorithm to factorize large biprimes and a triprime on ibm quantum computer," *arXiv preprint arXiv:1805.10478*, 2018.

6. APPENDIX

Here lists 1220 numbers out of 41654 in range from 5 to 10^{10} which satisfies the requirement of the use of circuits observed in our experiments.

[9003152533, 9008112889, 9004792969, 9008969713, 9013429921, 9010108993, 9014569489, 9015870467, 9020648401, 9003652249, 9027270947, 9037375969, 9016184329, 9037028201, 9043082089, 9044199013, 9044968193, 9045526691, 9003747761, 9027584689, 9039503153, 9048442001, 9031386409, 9032527081, 9050409769, 9057164881, 9016279577, 9062496361, 9072434417, 9071737033, 9084194773, 9084381347, 9086888809, 9004979353, 9099844289, 9011813953, 9107089093, 9107275907, 9097796153, 9105301993, 9094230289, 9120839509, 9025870993, 9098809249, 9122367973, 9122010361, 9121660817, 9123156769, 9124303249, 9034994929, 9106825201, 9124782769, 9129272161, 9112171129, 9135747493, 9136129909, 9136520513, 9128732969, 9140337013, 9120575041, 9151050373, 9136247209, 9148238633, 9160042691, 9119139857, 9166936547, 9178366369, 9178749673, 9190922281, 9103189633, 9197827729, 9188462873, 9105861673, 9011605649, 9191914769, 9197925073, 9013884233, 9203233001, 9206050691, 9207422929, 9017302649, 9203681593, 9115025929, 9210853909, 9118463713, 9198302929, 9222180707, 9126487729, 9198686641, 9037826753, 9224419969, 9139868929, 9212121601, 9233195297, 9143693929, 9238545721, 9049239113, 9220187281, 9057232049, 9157087729, 9229409521, 9252763433, 9235560241, 9236713729, 9260453893, 9069426721, 9073642057, 9075904129, 9076674473, 9082391993, 9083712067, 9083933161, 9086762371, 9081296537, 9086955077, 9086602177, 9088111313, 9091338787, 9081740209, 9082883881, 9003850979, 9099928801, 9006700961, 9007458181, 9102989969, 9104122757, 9010501609, 9011634661, 9012396161, 9008247169, 9098902849, 9015241379, 9009765841, 9109495537, 9016571749, 9107618657, 9112907689, 9113474371, 9018477073, 9019232777, 9019610629, 9113695777, 9095206313, 9118636609, 9105509513, 9034432501, 9130864321, 9010987873, 9125952161, 9131624741, 9131813827, 9029900329, 9035762243, 9014025793, 9038043779, 9111236033, 9131685161, 9134711497, 9042418549, 9045081349, 9130218649, 9142717729, 9046989673, 9048125029, 9048511609, 9146160481, 9006136297, 9004244281, 9031503769, 9128426393, 9149628217, 9152467747, 9001987777, 9013350217, 9062208709, 9135307073, 9153486977, 9159168197, 9039488473, 9063351109, 9160316741, 9006162937, 9015255001, 9063746009, 9065261353, 9117941257, 9166249987, 9021704753, 9069826069, 9118705201, 9169519913, 9170277889, 9172600777, 9006185401, 9077460713, 9078977209, 9080114581, 9174516457, 9176791201, 9131314897, 9007329433, 9084695209, 9182540161, 9183109027, 9003349027, 9082431409, 9003160921, 9004678313, 9005816357, 9017955493, 9090790309, 9182213177, 9006196201, 9018335849, 9085862641, 9091173737, 9140491057, 9186014737, 9017199137, 9018716689, 9020044547, 9092887043, 9190010371, 9178442881, 9002404097, 9096518113, 9052505489, 9098052209, 9006959021, 9011134753, 9029356129, 9102241633, 9103380469, 9188793169, 9028597817, 9055931033, 9092375321, 9103764161, 9104333603, 9153115801, 9189560089, 9201518371, 9013793417, 9014932613, 9158091577, 9016451989, 9063926489, 9033922993, 9039620053, 9106845361, 9112542421, 9161537137, 9209962147, 9029746529, 9035824033, 9102676577, 9163451617, 9025189937, 9119422993, 9025189997, 9027469973, 9035449889, 9027850081, 9120959009, 9101966569, 9123251273, 9174942697, 9036022403, 9042104131, 9078784553, 9224555971, 9039825859, 9048951907, 9040016177, 9041347171, 9049903561, 9134326609, 9231679313, 9233010307, 9052186849, 9132056569, 9042868787, 9053518531, 9135863873, 9233232961, 9235515049, 9048003617, 9114946273, 9137767633, 9230574497, 9051807577, 9133967929, 9054851513, 9117237769, 9214621193, 9235923817, 9191425801, 9240699427, 9196028377, 9243974401, 9244545187, 9057899029, 9125260273, 9243998737, 9246662741, 9236787169, 9245921857, 9150031249, 9109682489, 9134050873, 9152327161, 9063991829, 9134433169, 9157279009, 9158421301, 9136727113, 9209843017, 9252493961, 9162632629, 9211762537, 9115410089, 9139786153, 9158068201, 9161115209, 9163412513, 9251786881, 9073133813, 9118848533, 9167991857, 9265135637, 9075420161, 9084564833, 9171439217, 9079992737, 9268990561, 9076372891, 9087804931, 9121529449, 9267859561, 9086090737, 9088377289, 9078850073, 9081136769, 9083804581, 9101717033, 9102098149, 9126108457, 9126680131, 9088759921, 9091618531, 9102481249, 9103624693, 9126874721, 9271710961, 9086855429, 9132604709, 9096005993, 9097149797, 9109350373, 9132607721, 9274439417, 9111449987, 9281704009, 9282275971, 9107830009, 9135287641, 9284016481, 9097535017, 9118897673, 9143312137, 9100778179, 9103639669, 9146371253, 9281052049, 9293070307, 9121192481, 9145613089, 9147143281, 9295968841, 9108220393, 9295993177, 9109365673, 9141426457, 9152876737, 9153449251, 9202494617, 9299440321, 9107839189, 9125016409, 9143338777, 9121200929, 9127309153, 9152124713, 9136858693, 9296087641, 9159772249, 9162063457, 9297244729, 9115475609, 9115857493, 9138770533, 9309472681, 9116621357, 9140300149, 9162069361, 9164742773, 9164933731, 9305669777, 9310252769, 9311398517, 9138391481, 9139919209, 9140683073, 9141255971, 9165126721, 9309497017, 9311788609, 9127508483, 9133620931, 9170295619, 9316994371, 9125789837, 9126554053, 9137253077, 9149862641, 9320664917, 9126936209, 9137635681, 9318762457, 9321055201, 9321628387, 9138400889, 9321835769, 9132668969, 9134197753, 9177768097, 9132669209, 9139550177, 9176248673, 9323042657, 9137256857, 9147197281, 9307008713, 9329948153, 9150258049, 9331509961, 9335537347, 9167088641, 9179327617, 9144523093, 9181627177, 9193485173, 9328513321, 9340371317, 9182393761, 9329286049, 9155044163, 9332763721, 9160212617, 9183180857, 9201555449, 9161361161, 9162126817, 9162701059, 9208066177, 9257833817, 9331336793, 9197732161, 9258988481, 9353935777, 9163658513, 9164232851, 9211711459, 9164998747, 9188931497, 9207311849, 9210375241, 9335974313, 9348227881, 9360289987, 9213058721, 9360876649, 9179552131, 9191807747, 9314555401, 9173999897, 9175149173, 9195453049, 9270539081, 9367844449, 9174957787, 9370355107, 9176681989, 9196989257, 9370942081, 9177065173, 9187410601, 9187985347, 9200055013, 9323050657, 9183196457, 9373265641, 9189711169, 9190285987, 9201207529, 9276317081, 9373652929, 9374227747, 9376751521, 9211570129, 9378744737, 9202369441, 9289035017, 9203903873,

9199495387, 9200070853, 9204674581, 9392276497, 9201221893, 9499417009, 9504090721, 9483838081, 9504870649, 9482864399,
9347399401, 9396125237, 9201797467, 9205826233, 9348559657, 9501366409, 9529411561, 9526685849, 9529802041, 9502926073,
9385394089, 9300604337, 9386556721, 9397300769, 9208129537, 9510719653, 9494163619, 9540342121, 9540731813, 9529822777,
9396185657, 9401558689, 9226169593, 9210816533, 9211008451, 9546593333, 9535680937, 9503714593, 9504884149, 9520868081,
9231159841, 9232311349, 9392370961, 9398512337, 9403910377, 9536462161, 9545818609, 9548742499, 9506249999, 9508394977,
9406789507, 9213696143, 9231933673, 9235005257, 9360940201, 9543494617, 9555779491, 9555975509, 9509565253, 9523218473,
9232318009, 9404330297, 9230401781, 9365972137, 9414746741, 9535506371, 9515612303, 9516782867, 9517758337, 9518343619,
9366746401, 9371779897, 9235399897, 9238858561, 9242703721, 9521465123, 9527708131, 9565166179, 9516977989, 9518538773,
9329559137, 9403347809, 9427559717, 9425289857, 9389989201, 9521660341, 9527903477, 9565362293, 9519709697, 9522831649,
9426905809, 9248476417, 9249245893, 9249438227, 9251169233, 9529075553, 9566538977, 9520685467, 9569861251, 9524393393,
9444849571, 9250592399, 9253477769, 9423141113, 9435452281, 9530638321, 9568107889, 9570449737, 9527712091, 9533763857,
9446224553, 9255401989, 9453404227, 9443613889, 9449772161, 9539229961, 9571245713, 9582198721, 9548021827, 9545484617,
9455737987, 9268682851, 9314887171, 9267142747, 9269453059, 9577521361, 9567757841, 9553302181, 9572453537, 9597272131,
9272340949, 9291015971, 9364753429, 9268875589, 9270030817, 9606098521, 9607274689, 9562492943, 9612168739, 9609627241,
9273496501, 9291595073, 9274652449, 9275422697, 9281584681, 9612365333, 9568947977, 9570121733, 9572077993, 9571687189,
9317790241, 9278119429, 9293911481, 9278698267, 9279468851, 9573643769, 9595166149, 9596343121, 9573839707, 9577166513,
9281010019, 9370590409, 9280046873, 9281588137, 9291221281, 9583428721, 9586364131, 9598888547, 9585385889, 9576579599,
9291799267, 9322817849, 9282358961, 9286983137, 9300091369, 9579515609, 9579907093, 9603396133, 9580690157, 9586562897,
9310114577, 9334787089, 9384132113, 9299708969, 9318221417, 9593414947, 9604573609, 9610064417, 9590089037, 9595572949,
9395163779, 9300094933, 9304337897, 9304916483, 9345224641, 9614374933, 9593418691, 9595964897, 9614767649, 9595769539,
9385339937, 9394597313, 9397490243, 9322855481, 9325748771, 9601843337, 9622416707, 9611249273, 9622222249, 9604391779,
9338286361, 9350438179, 9399238337, 9303374107, 9321313993, 9620265673, 9630070313, 9609096451, 9629678761, 9637922053,
9305496209, 9317071529, 9308969093, 9324790009, 9398878201, 9617528617, 9634793513, 9638329601, 9644414467, 9650703683,
9326721409, 9332510149, 9357401731, 9406606021, 9406798979, 9659547893, 9672131509, 9671738449, 9690616081, 9691009849,
9310320091, 9334055893, 9358949539, 9357215689, 9359531521, 9674098549, 9674295203, 9680588131, 9718345699, 9768492469,
9359917493, 9403532329, 9334830289, 9320357539, 9323253349, 9768689123, 9681573721, 9683934049, 9684524131, 9695347009,
9323446403, 9415919269, 9416112323, 9326344073, 9419038793, 9680198543, 9703614649, 9704992067, 9730179139, 9774453289,
9421742389, 9329241743, 9330400787, 9421772089, 9427760483, 9780553283, 9686692217, 9705189349, 9724473593, 9730376933,
9330593989, 9422160361, 9427955701, 9356483057, 9405942769, 9774848761, 9779571433, 9780752101, 9684331277, 9685118533,
9424490161, 9429127009, 9391292777, 9392452709, 9417584569, 9696336931, 9731173009, 9778408369, 9685512209, 9694172377,
9347408899, 9393229057, 9393809059, 9351082501, 9443499977, 9779199481, 9730391273, 9733540681, 9736493251, 9707166409,
9375064241, 9387441457, 9396724369, 9357272389, 9376226177, 9711891001, 9735513961, 9693386881, 9693977539, 9740639521,
9400788739, 9448946833, 9406219171, 9431175769, 9454010273, 9741230179, 9730799161, 9781207097, 9698900713, 9719183267,
9401773193, 9361142993, 9460609189, 9411072617, 9460615273, 9743798017, 9696340891, 9743014249, 9744198769, 9699295189,
9366949073, 9371982337, 9375467029, 9468004961, 9372369577, 9722930149, 9724114921, 9753867619, 9803712161, 9804303203,
9372756773, 9374692753, 9380887889, 9393278161, 9398704933, 9724909009, 9731017187, 9805300513, 9752894873, 9756047929,
9470352473, 9471901609, 9473063461, 9375080621, 9473452789, 9758806853, 9748563361, 9758023489, 9760979779, 9799017377,
9387668131, 9400061987, 9473844161, 9474425123, 9385539617, 9810842537, 9811236709, 9727083907, 9719002081, 9730835449,
9391544131, 9397936033, 9380697307, 9477742009, 9430869233, 9735569257, 9728665907, 9777584899, 9732019657, 9732611491,
9397555177, 9409957481, 9393292417, 9397750403, 9404146529, 9779958211, 9830461379, 9755298977, 9774238049, 9778972817,
9415775849, 9441360353, 9490203497, 9490591141, 9404537953, 9805803169, 9734979547, 9784705699, 9810160753, 9829104049,
9412294193, 9421601681, 9486754097, 9497612833, 9405701713, 9782932681, 9785300737, 9833451209, 9836213941, 9744453787,
9407059139, 9425675267, 9498782353, 9406090081, 9406477973, 9749981603, 9832306577, 9843362209, 9844744163, 9745835777,
9423546409, 9502681273, 9419280713, 9431307349, 9456524489, 9746625481, 9843759073, 9750574241, 9845342561, 9748205273,
9505794901, 9408805997, 9507354949, 9502314961, 9507747017, 9797174857, 9823239313, 9845354609, 9798163171, 9774271841,
9411716147, 9432087617, 9434803813, 9503484769, 9431702473, 9797968721, 9758871173, 9850927609, 9856853989, 9760254211,
9512035861, 9428212201, 9432486337, 9497719393, 9521016913, 9807668131, 9856860073, 9856486561, 9859648193, 9861229009,
9434040337, 9499278769, 9430352051, 9431323081, 9503567713, 9800765137, 9813214819, 9857677969, 9863804003, 9807484913,
9528037669, 9443754197, 9512928769, 9534690593, 9440648533, 9810646801, 9839103793, 9862817953, 9774682789, 9793659493,
9441037189, 9442591733, 9514489393, 9538973461, 9442786267, 9819357113, 9774881423, 9775276891, 9777847433, 9780813443,
9443757977, 9540151609, 9541722473, 9548358073, 9456589829, 9784174921, 9787140931, 9872759753, 9775474637, 9781011301,
9553042981, 9530493169, 9554608937, 9509109689, 9555794009, 9786152489, 9787338917, 9798807721, 9874739113, 9781407017,
9492004453, 9480133987, 9517498339, 9478384549, 9481888321, 9787734889, 9875534113, 9779232091, 9779825413, 9791098531,
9484808131, 9497071333, 9480916891, 9483253699, 9503700769, 9797625073, 9803558293, 9879503509, 9791692609, 9792088181,

9799604833, 9804351889, 9831251873, 9783979171, 9787341737,
9804747961, 9875955241, 9880702393, 9806728441, 9883877461,
9784968497, 9786155429, 9794463953, 9802376833, 9878340481,
9787738453, 9796048321, 9799016131, 9805545313, 9811678787,
9837201953, 9793278497, 9798027089, 9807922009, 9890041379,
9791102491, 9796644259, 9882346217, 9893430073, 9798426133,
9800405753, 9803177221, 9809907929, 9822181573, 9885925337,
9804365713, 9823372369, 9822977777, 9825749749, 9899009009,
9803970221, 9806346533, 9806742697, 9855062993, 9808525219,
9830706371, 9828135553, 9824175593, 9833684681, 9817044557,
9819620611, 9822592981, 9822989537, 9823386193, 9822990257,
9824179493, 9824377699, 9833296969, 9897515713, 9834883397,
9898709593, 9825765589, 9825963827, 9830721539, 9827153423,
9838850881, 9839445667, 9877710233, 9832110073, 9839644181,
9903485833, 9904680073, 9832903777, 9881288489, 9846392137,
9851352547, 9847981973, 9921406993, 9851356507, 9855128273,
9857114053, 9914716793, 9870025103, 9872806819, 9875985923,
9873005573, 9874992553, 9876184741, 9874198157, 9924477859,
9887116387, 9925274851, 9878968193, 9883341649, 9888112417,
9903617413, 9926278561, 9929260291, 9880161197, 9880956373,
9881354009, 9896069137, 9905614513, 9900047401, 9900445157,
9896867093, 9900050101, 9919148149, 9935866177, 9947804617,
9902836913, 9921940337, 9937859857, 9905424667, 9943044361,
9949413833, 9924732913, 9925131409, 9913388131, 9923144129,
9912392717, 9913189189, 9913587473, 9914184851, 9935093081,
9938079971, 9914981467, 9939477409, 9953816497, 9929121929,
9941071649, 9941469973, 9921952877, 9923148161, 9927530869,
9932710433, 9934104931, 9927929537, 9934305937, 9935105429,
9946068931, 9959025641, 9938694053, 9938893411, 9949859401,
9941685263, 9954048931, 9953849761, 9954248597, 9945275027,
9949463813, 9952655269, 9972202937, 9955449473, 9957045649,
9959639843, 9960438979, 9960239537, 9966228557, 9976613113,
9983004089, 9977212771, 9986201161, 9975814637, 9986203861,
9987802697, 9985205467]